НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет електроніки
(повна назва інституту/факультету)

Кафедра звукотехніки та реєстрації інформації
(повна назва кафедри)

«На правах рукопису»
УДК 004.7:654.195.6

«До захисту допущено»

Завідувач кафедри
_____ ГГ. Власюк
(підпис) (ініціали, прізвище)
“___”_____ 2018р.

Магістерська дисертація

зі спеціальності 171 Електроніка
(код і назва спеціальності)

на тему: “Шляхи удосконалення безпроводових мереж у місцях великого скупчення людей”.

Виконав : студент VI курсу, групи ДВ-72мп
(шифр групи)

Лавренюк Володимир Іванович _____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник доцент к.т.н., доцент Лазебний В.С _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018 року

Національний технічний університет України
«Київський політехнічний інститут
імені Ігоря Сікорського»

Інститут/факультет _____Факультет електроніки_____
(повна назва)

Кафедра _____Звукотехніки та реєстрації інформації_____
(повна назва)

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою

Спеціальність (спеціалізація) 171 Електроніка (Електронні та інформаційні технології кінематографії та аудіовізуальних систем_____
(код і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ ГГ. Власюк
(підпис) (ініціали, прізвище)
«___»_____2018 р.

ЗАВДАННЯ
на магістерську дисертацію студенту
_____Лавренюку Володимиру Івановичу_____
(прізвище, ім'я, по батькові)

1. Тема дисертації "Шляхи удосконалення безпроводових мереж у місцях великого скупчення людей".
науковий керівник дисертації Лазебний Володимир Семенович, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом по університету від «07» листопада 2018 р. № 4114-с
2. Строк подання студентом дисертації 10.12.2018 р.
3. Об'єкт дослідження: безпроводові мережі Wi-Fi та мобільного зв'язку 3, 4, 5 поколінь.

4. Предмет дослідження (Вихідні дані – для магістерської дисертації за освітньо-професійною програмою) принципи функціонування безпроводових мереж у місцях великого скупчення людей.

5. Перелік завдань, які потрібно розробити: 1) Проаналізувати принципи функціонування Wi-Fi мережі, особливості використання та рекомендації щодо організації мережі; 2) Дослідити принципи побудови мереж мобільного зв'язку 3, 4, 5 поколінь, та розробити рекомендації щодо їх планування; 3) Проаналізувати принципи безпеки у безпроводових мережах 4) Розробити стартап проект.

6. Перелік графічного (ілюстративного) матеріалу 27 рис., 25 табл., 1 презентація , 12 слайдів.

7. Орієнтовний перелік публікацій 1) Побудова мережі Wi-Fi на стадіоні /Лавренюк В.І.// Науково-технічна конференція студентів, аспірантів та науковців “ Сучасні проблеми застосування електронних та інформаційних технологій в телекомунікаціях, телебаченні та цифровому кінематографі ”; 2) Шляхи вдосконалення безпроводових мереж у місцях великого скупчення людей/ Лавренюк В.І.// XI Міжнародна науково-технічна конференція молодих вчених «Електроніка-2018».

8. Консультанти розділів дисертації*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання 10.09.2017

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів магістерської дисертації	Примітка
1	Написання першого розділу “Дослідження технологій стандарту ieee 802.11 як засобу забезпечення доступу до інформаційних ресурсів”	06.11.2017-27.11.2017	
2	Написання другого розділу “Дослідження мереж 3,4,5 покоління, як засобів забезпечення доступу до інформаційних ресурсів”	05.02.2018-26.02.2018	
3	Написання третього розділу “Захист інформації в безпроводових мережах і його вплив на якість надання інформаційних послуг”	07.05.2018-28.05.2018	
4	Написання четвертого розділу “ Розроблення стартап-проекту ”	01.11.2018-19.11.2018	
5	Підготовка матеріалів до друку та оформлення пояснювальної записки	05.12.2018	
6	Підготовка презентації для виступу	10.12.2018	

Студент _____ Лавренюк В.І
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ Лазебний В.С.
(підпис) (ініціали, прізвище)

* Консультантом не може бути зазначено наукового керівника

УДК 004.7:654.195.6

РЕФЕРАТ

Магістерська дисертація: 95 с. 27 рис., 25 табл., 1 дод., 15 джерел.

БЕЗПРОВОДОВА МЕРЕЖА, WI-FI, ТЕЛЕКОМУНІКАЦІЯ, ВИСОКА ЩІЛЬНІСТЬ, БЕЗПЕКА.

Метою дисертації є дослідження шляхів удосконалення мереж безпроводового зв'язку, щоб з'ясувати які умови необхідні для роботи мереж у місцях високої щільності.

Об'єктом дослідження є безпроводові мережі Wi-Fi та мобільного зв'язку 3, 4, 5 поколінь.

Результатом роботи є формування об'єктивних оцінок щодо можливості використання безпроводових технологій у місцях великого скупчення людей, з'ясовано можливості захисту безпроводових мереж від несанкціонованого доступу до інформаційних ресурсів, досліджено архітектуру мережі Wi-Fi та мобільного зв'язку 3, 4, 5 поколінь.

Результати роботи будуть корисними для фахівців, що працюють у сфері мобільного зв'язку. Результати можна використати під час планування та введення в експлуатацію Wi-Fi мережі та мереж 3,4,5 покоління, а також у навчальному процесі під час підготовки фахівців у сфері телекомунікацій.

Результати дослідження та публікації були оприлюднені на конференції молодих вчених "Електроніка 2018" та на науковій-технічній конференції студентів, аспірантів та науковців "Сучасні проблеми застосування електронних та інформаційних технологій в телекомунікаціях, телебаченні та цифровому кінематографі".

SUMMARY

Master’s dissertation: 95 p., 27 pic., 25 tab., 1 add., 15 sour.

WIRELESS NETWORK, WI-FI, TELECOMMUNICATION, HIGH DENSITY, SAFETY.

The aim of the work is research on ways to improve wireless networks to find out what conditions are needed for networks in high density areas.

The object of research is wireless network: Wi-Fi, 3,4,5 G.

The result of the work is the formation of objective assessments of the possibility of use wireless technologies in areas with large concentrations of people, found out the possibility of protecting wireless networks from unauthorized access to information resources, have investigated network architecture Wi-Fi, 3,4,5 G.

The results of the work will be useful for specialists working in the field of mobile communication. The results can be used in the planning and commissioning of Wi-Fi networks and 3,4,5 generation networks, as well as in the educational process in the preparation of specialists in the field of telecommunications.

The results of the research and publications were published at the conference of young scientists "Electronics 2018" and at the scientific and technical conference of students, postgraduates and scientists "Modern problems of application of electronic and information technologies in telecommunications, television and digital cinema".

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

DSSS – Direct Sequence Spread Spectrum (метод прямої послідовності для розширення спектру);

DCF – Distributed coordination function (розподілена функція координації);

PCF – Point coordination function (функція координації точок);

PC – Point Coordination (точка координації);

RTS – Request to Send (запит на передачу);

CTS – Clear to Send (підтвердження готовності);

OFDM – Orthogonal Frequency Division Multiplexing (ортогональне частотне мультиплексування) ;

MIMO – Multiply Input Multiply Output (множинний вхід, множинний вихід) ;

QAM – Quadrature Amplitude Modulation (квадратурно-амплітудна модуляція) ;

BSS – Base Station Subsystem (підсистема базових станцій) ;

WPA2 – Wi-Fi Protected Access (Wi-Fi захищений доступ) ;

QoS – Quality of service (якість обслуговування) ;

SSID – Service Set Identifier (ідентифікатор набору служб) ;

CDMA – Code Division Multiple Access (множинний доступ з кодовим розділенням каналів) ;

UMTS – Universal Mobile Telecommunications System (універсальна мобільна телекомунікаційна система) ;

GSM – Global System for Mobile Communications (глобальна система мобільного зв’язку) ;

SGSN – Serving GPRS Support Node (вузол обслуговування абонентів

GPRS) ;

MSC – Mobile Switching Centre (центр мобільної комутації) ;

MGW – Media gateway (медіашлюз) ;

RNC – Radio Network Controller (контролер мережі радіодоступу) ;

WiMAX – Worldwide Interoperability for Microwave Access (загальносвітова сумісність широкосмугового безпроводового доступу) ;

E-UTRAN – Evolved UMTS Terrestrial Radio Access Network (розвинута мережа наземного радіозв'язку UMTS);

SAE – System Architecture Evolution (еволюція системної архітектури)

eNB – Evolved Node B (розвинутий вузол);

MME – Mobility Management Entity (організація з управління мобільністю);

MMO – Mobility Management Entity (вузол управління мобільністю) ;

RRM – Radio Resource Management (управління радіоресурсами) ;

PSK – Pre-Shared Key (фазова маніпуляція) ;

KRACK – Key Reinstallation Attacks (повторне використання ключа) ;

IEEE – Institute of Electrical and Electronics Engineers (Інститут інженерів з електротехніки та електроніки).

ВСТУП

Перш за все необхідно відзначити, що сучасні підходи проектування мереж з високою щільністю ґрунтуються на розумінні того, що основний користувач в такому сценарії це людина з мобільним пристроєм. Загальна кількість присутніх людей в таких місцях дуже велика, тому кількість потенційних користувачів мережі Wi-Fi також може бути великою.

Сьогодні корпоративні клієнти все частіше вибирають безпроводові мережі. Це зручно тому, що не потрібно розгортати класичні кабельні мережі. При цьому пропускна спроможність, що забезпечується безпроводовими установками, може реально конкурувати з пропускною спроможністю проводових мереж. Тому можна стверджувати, що тема магістерської дисертації є **актуальною**.

Метою дисертації є дослідження шляхів удосконалення мереж безпроводовго зв'язку, щоб з'ясувати які умови необхідні для роботи мереж у місцях високої щільності.

Для досягнення поставленої мети в роботі необхідно було виконати такі **завдання**:

− проаналізувати принципи функціонування Wi-Fi мережі, особливості використання та рекомендації щодо організації мережі;

− дослідити принципи побудови мереж мобільного зв'язку 3, 4, 5 поколінь, та розробити рекомендації щодо їх планування;

− проаналізувати принципи безпеки у безпроводових мережах;

− розробити стартап проект.

Об'єктом дослідження є безпроводові мережі Wi-Fi та мобільного зв'язку 3, 4, 5 поколінь.

Предмет дослідження – принципи функціонування безпроводових мереж у місцях великого скупчення людей.

Методом дослідження є критичний аналіз принципів організації та

функціонування безпроводових мереж, порівняльний аналіз особливостей використання в місцях високої щільності, та шляхи удосконалення цих мереж.

Новизна дослідження полягає у розробленні детального алгоритму дій, що дозволить початківцю самостійно провести весь технологічний етап планування безпроводових мереж.

Практична цінність полягає у висвітленні технічних аспектів, які необхідно враховувати при проведенні планування безпроводових мереж у місцях великого скупчення людей за умови використання відповідних апаратних і програмних засобів

1 ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ СТАНДАРТУ IEEE 802.11 ЯК ЗАСОБУ ЗАБЕЗПЕЧЕННЯ ДОСТУПУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ

1.1 Принципи функціонування безпроводових локальних мереж стандарту IEEE 802.11

Проаналізуємо детальніше, що містить стандарт IEEE 802.11, як центральний для всіх наступних специфікацій. Так як і всі стандарти IEEE 802, в документі IEEE 802.11 розглядаються два рівня моделі об'єднування відкритих систем (OSI): канальний (Data Link Layer) та фізичний. Причім перший розділяється на два підрівня. Верхній – Logical Link Control (LLC) відтворений в стандарті IEEE 802.2.

Стандарт IEEE 802.11 простежує лишень нижній підрівень Medium Access Control (MAC), іншими словами управління доступом до каналу. Тобто, на фізичному рівні стандарт передбачає спосіб роботи з середовищем передавання, методи та швидкість модуляції. На MAC рівні – спосіб, за допомогою якого пристрої застосовують (ділять) загальний канал, принципи підключення пристроїв до ТД і їх автентифікації, операції захисту даних. Через те, що стандарт IEEE 802.11 створювався як «безпроводовий Ethernet», який визначає 48-бітну пакетну передачу з адресами пакетів, як і всяка мережа Ethernet. Комітет IEEE 802 зокрема приділяв увагу сумісності всіх своїх стандартів, в наслідок безпроводові та проводові мережі IEEE 802 просто сполучаються один з одним.

Коли говориться про радіотракт, основне питання – частотний діапазон. IEEE 802.11 зв'язаний з існуючими в США і ряді інших країн безліцензійних частотних діапазонів. Спочатку він був спрямований на діапазон 2,400 – 2,4835 ГГц з шириною смуги 83,5 МГц. Спектральна маска для одного каналу наведена на рис. 1.1 (потужність відраховується щодо піків функції sin (x)/x). Ширина канала за рівнем -30 дБ становить 22 МГц, отже, в смузі 83,5 МГц можливо три неперекриваючі канали.

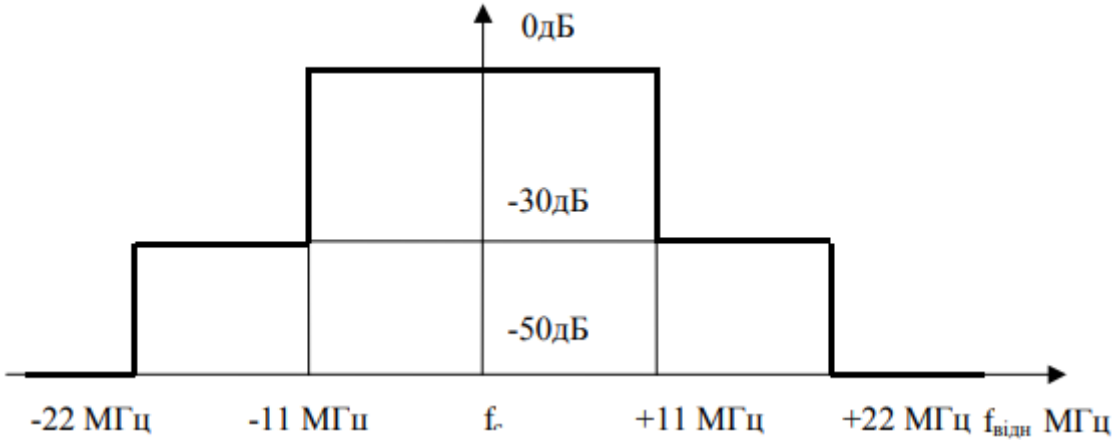

Рисунок 1.1 – Спектральна маска каналу мережі 802.11 з модуляцією методом DSSS

Стандарт визначає два основних засобів організації локальної мережі: за способом «рівний з рівним» (Ad-hoc мережа рис. 1.2, а) і у вигляді структурованої мережі (рис. 1.2, б).

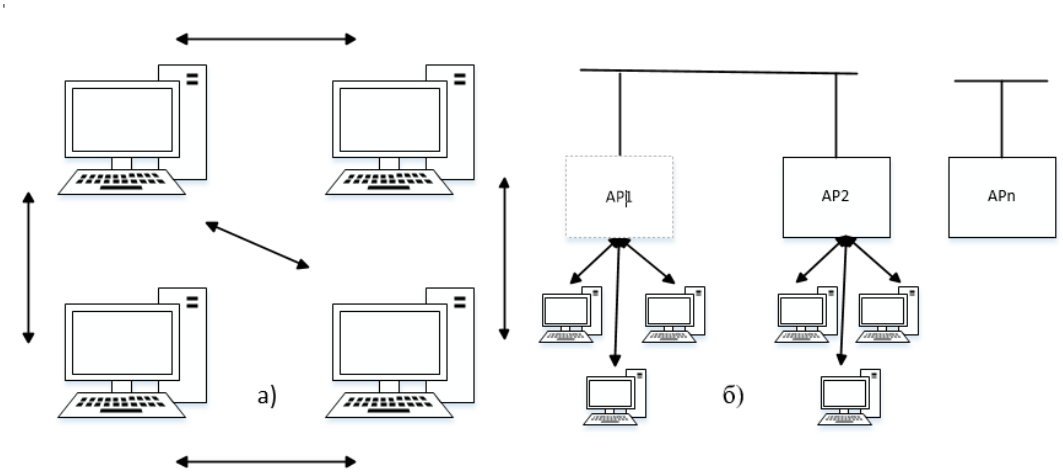

Рисунок 1.2 – Архітектура мережі 802.11: а) ad-hoc-мережа; б)структуровані мережі

У найпершому випадку зв’язок встановлюється практично між двома станціями, і жодного адміністрування не передбачено. У випадку структурованих мереж (а як розкриває практика, це головний спосіб спорудження мереж IEEE 802.11) в їх складі з’являється допоміжний пристрій –

точка доступу (AP – Access Point), як правило, стаціонарна і дієвий на фіксованому каналі.

Зв’язок між пристроями створюється тільки через AP. Через них же імовірний вихід в зовнішні провідні мережі. У мережі IEEE 802.11 може бути кілька AP, об’єднаних мережею Ethernet. У дійсності така мережа становить набір базових станцій з перекриваючими зонами охоплення. Стандарт IEEE 802.11 припускає переміщення пристроїв із зони однієї AP в зону іншої (роумінг), у такий спосіб забезпечуючи мобільність. Адже для мобільних станцій основне питання ресурсу елементів живлення, в стандарт закладений спеціальний протокол управління енергоспоживанням – безпосередньо при обміні передавальний пристрій може перевести приймач в режим очікування.

Основна вимога до стандартів безпроводового зв’язку – безпека передачі даних. У зв’язку з цим на MAC-рівні передбачений принцип захисту даних, що поєднує автентифікацію станцій та шифрування переданих даних. Описаний принцип має забезпечувати такий же рівень захисту, як і в звичайних мережах Ethernet, із-за чого його назвали WEP (Wired Equivalent Privacy – еквівалент провідної конфіденційності). Алгоритм WEP заснований на застосуванні чотирьох загальних для однієї мережі секретних ключів довжиною 40 біт. Саме шифрування виконується за алгоритмом RC4 компанії RSA Security. Алгоритм застосовує перемноження блоків вихідних даних на псевдовипадкову послідовність такої ж довжини, що і блок шифрованих даних. Генератор псевдовипадкової послідовності ініціалізується 64-разрядним числом, що складається з 24-розрядного вектора ініціалізації (IV – initialization vector) і 40-розрядного секретного ключа. Суттєво, що якщо секретний ключ відомий пристроям і незмінний, то вектор IV може змінюватися від пакету до пакету. Для захисту від несанкціонованої зміни переданої інформації кожен шифрований пакет захищається 32-розрядною контрольною сумою (ICV-integrity check value). Тобто, при шифруванні до переданих даних додається 8 байт: 4 для ICV, 3 для IV, і ще 1 байт має інформацію про номер використовуваного секретного ключа (одного із чотирьох). Зазначимо, що

секретний ключ може бути набагато довшим - 64, 128 біт тощо. Це не суперечить стандарту, більш того, таке обладнання випускається, але законодавство США перешкоджає експорту пристроїв, що підтримують шифрування даних з ключем довше 40 біт. Саме тому виробники і обмежуються 240 варіантами ключа. Додаткові методи захисту інформації і автентифікації в мережах 802.11 описані в стандарті IEEE 802.11.

Як ми вже відзначали, пристрої, відповідні вихідної специфікації IEEE 802.11, практично не отримали розвитку. Надалі будемо розглядати IEEE 802.11 з точки зору специфікації IEEE 802.11 b, як найпершої, активно підтриманої виробниками апаратури.

MAC рівень стандарту IEEE 802.11. Стандарт IEEE 802.11 визначає два режими керування мережею: коли функції управління розподілені між всіма пристроями мережі IEEE 802.11 – так званий режим DCF (Distributed coordination function) – і коли вони сконцентровані в одній певній точці доступу – режим PCF (Point coordination function). В режимі DCF всі пристрої працюють за способом конкурентного доступу до каналу передачі, себто пріоритетів не існує. Потрібність в режимі централізованого управління PCF появляється за передачі чутливої до затримок інформації, коли потрібно запровадити пріоритети доступу.

Функціонування в режимі PCF може відбуватися лишень під управлінням спеціальної точки доступу, званої точкою координації (PC), і тільки в певні, періодично повторювані інтервали. Коли мережа переходить в режим PCF, в трафіку з’являються інтервали, в яких конкурентний доступ скасовано, і цілий обмін досягається під управлінням координуючого пристрою (PC) (рис. 1.3). При закінченні такого інтервалу мережа трансформується в режим DCF. Інтервали під управлінням PC рухаються через строго вивірений період, на початку кожного інтервалу PC виставляє вагомий сигнальний кадр (Beacon). PC не може передати черговий сигнальний кадр до тих пір, поки канал не звільниться, себто черговий «вільний від конкуренції» інтервал може розпочатися з затримкою.

Режим PCF вагомий для передачі, регулярно повторюваної чутливої до затримок інформації. Він також результативний, якщо мережа IEEE 802.11 використовуються в якості середовища доступу до Інтернету (або іншим глобальним мережам), тобто забезпечують обмін даними між користувачами і централізованим провайдером. Однак головний принцип мереж Ethernet це все ж довільний конкурентний доступ, що і робить останніми настільки простими в реалізації та експлуатації. В проводових мережах Ethernet застосовується механізм з контролем несучої множинного доступу до каналу зв'язку та виявленням суперечок (CSMA/CD – Carrier Sense Multiple Acsses with Collision Detection). Станція може розпочати передачу, тоді коли канал вільний. Якщо станції розкривають, що на одному каналі намагаються діяти кілька станцій, всі вони зупиняють передачу і намагаються відновити її через випадковий проміжок часу. Тобто, навіть при передачі пристрій має контролювати канал, таким чином працювати на прийом.

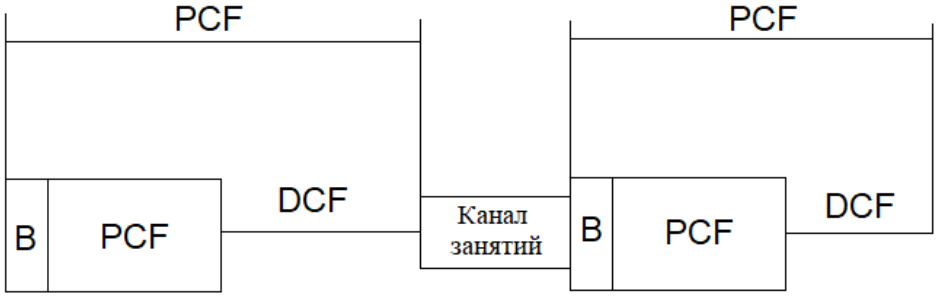

Рисунок 1.3 – Цикли роботи мережі в режимах з: централізованим (PCF) і розподіленим (DCF) управлінням

Те, що відносно просто при проводовому зв'язку, проблематично в безпроводових комунікаціях – загасання сигналу в ефірі набагато потужніше, ніж у проводі. Тому виникають дві основні проблеми. По-перше, досить складне, якщо взагалі вирішуване, завдання контролю несучої передавальним пристроєм (коли воно віщає, то власний сигнал свідомо набагато потужніше, ніж сигнал віддаленого пристрою). По-друге, вірогідна ситуація, коли два

пристрої видалено і не чують один одного, проте обидва потрапляють в зону охоплення третього пристрою – так звана проблема прихованих станцій. Якщо обидва пристрої, A та B розпочинають передачу, то вони принципово не зможуть виявити суперечну ситуацію і виявити, чому пакети не проходять.

Для виключення подібних проблем в специфікації IEEE 802.11 прийнятий механізм CSMA/CA (Carrier sense Multiple Acsses with Collision Avoidance) множинний доступ з контролем несучої і запобіганням колізій. Перед початком передачі пристрій слухає ефір і очікує, коли канал звільниться. Канал визначається вільним, якщо не виявлено активності протягом деякого проміжку часу – між кадрового інтервалу (IFS) певного типу. Якщо протягом цього проміжку канал залишався вільним, пристрій очікує ще протягом випадкового часу відстрочки і, якщо канал ще не зайнятий, передає пакет. Якщо пакет призначений конкретному пристрою (не широкомовна або багатоадресна передача), то приймач, успішно прийнявши пакет, посилає передавачу короткий кадр підтвердження отримання АСК (ACKnowledge). Якщо передавач не прийняв АСК, він вважає відісланий пакет загубленим і повторює процедуру його передачі.

Примітно, що, якщо пристрій повторно передає пакет, для визначення незайнятості каналу, він повинен використовувати збільшений міжпакетний інтервал (EIFS). Крім того, час відстрочки вибирається випадковим чином на деякому інтервалі. При першій спробі передачі цей інтервал мінімальний. При кожній наступній він подвоюється до тих пір, поки не досягне заданого граничного значення. Ці заходи призводять до того, що пристрій, успішно передав пакет, має переваги в захопленні каналу (хто помиляється, той довше чекає).

Перед першою спробою отримати доступ до каналу пристрій завантажує тривалість випадкового інтервалу відстрочки в спеціальний лічильник. Його значення декрементується із заданою частотою, поки канал вільний. Як тільки лічильник обнулиться, пристрій може займати канал. Якщо до обнулення лічильника канал займає інший пристрій, рахунок зупиняється, зберігаючи

досягнуте значення. При наступній спробі відлік починається зі збереженої величини. В результаті, який не встиг минулого разу отримує більше шансів зайняти канал в наступний. У провідних мережах Ethernet подібного механізму немає.

Однак описані процедури доступу не позбавляють від проблеми прихованих станцій. Для її подолання використовуються два додаткових кадра: RTS (Request to Send – запит на передачу) і CTS (Clear to Send – підтвердження готовності). Пристрій, що бажає відправити пакет даних, передає адресату короткий кадр RTS. Якщо приймальний пристрій готовий до прийому, він виставляє передавальному відповідний кадр – CTS. Далі відповідно до описаної вище процедур передавальний пристрій відправляє кадр з даними і чекає підтвердження АСК.

Стандарт IEEE 802.11 передбачає два механізми контролю за активністю в каналі (виявлення несучої): фізичний та віртуальний. Перший механізм реалізований на фізичному рівні і зводиться до визначення рівнів сигналу в антені і порівнянні його з пороговою величиною. Віртуальний механізм виявлення несучої заснований на тому, що в переданих кадрах даних, а також у керівних кадрах АСК і RTS/CTS міститься інформація про час, необхідний для передачі пакета (або групи пакетів) і отримання підтвердження. Всі пристрої мережі приймають інформацію про поточну передачу і можуть визначити, скільки часу канал буде зайнятий, тобто пристрій при встановленні зв’язку всім повідомляє, на який час він резервує канал.

Як ми вже говорили, весь обмін в мережах IEEE 802.11 відбувається за допомогою окремих кадрів (frames). За їх структурою особливо чітко видно поділ на фізичний і MAC-рівні. Фактично кадр формується на MAC-рівні, на фізичному рівні до нього додається заголовок фізичного рівня (PLCP). На MAC-рівень пакети передаються від додатків верхнього рівня. Якщо їх розмір перевищує максимально допустимий в IEEE 802.11, відбувається дефрагментація, великий пакет розбивається на кілька менших, які передаються за спеціальною процедурою.

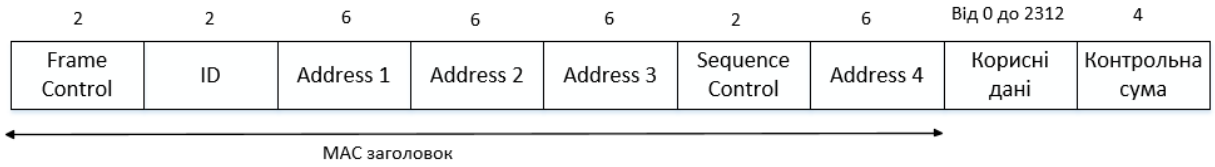

Рисунок 1.4 – Структура кадрів MAC-рівні мережі 802.11

Кадри MAC-рівня можуть бути трьох типів: кадри даних, контрольні (ACK, RTS, CTS) і кадри управління (наприклад, Beacon). Їх структура однакова (рис. 1.4). Кожен MAC-кадр включає MAC-заголовок, поле даних (Frame Body) і контрольну суму CRC. У заголовку передається повна інформація про версію протоколу стандарту групи IEEE 802.11, типу кадру, системи захисту (поле Frame Control); тривалості процедури передачі пакету (Duration/ID), адреси одержувача/відправника (Address L-4; чотири адресних поля необхідні, якщо пакети передаються з підмережі однієї точки доступу в підмережу іншій) і інформація про послідовність пов’язаних пакетів (Sequence Control). Поле даних може бути різної довжини або зовсім відсутні (в контрольних кадрах) [1].

Збільшення швидкості до 54 Мбіт/с було реалізовано в стандарті 802.11a (даний стандарт почав розроблятися раніше, ніж стандарт 802.11 , але фінальна версія була випущена пізніше). Збільшення швидкості в основному було досягнуто за рахунок збільшення глибини модуляції до 64 рівнів на один символ. Крім того, була радикально переглянута радіочастотна частина: розширення спектру методом прямої послідовності було замінено на розширення спектру методом послідовного поділу сигналу на паралельні ортогональні підносійні (OFDM). Використання паралельної передачі на 48 підканалах дозволило знизити міжсимвольну інтерференцію за рахунок збільшення тривалості окремих символів. Передача даних здійснювалася в діапазоні 5 ГГц. При цьому ширина одного каналу становить 20 МГц.

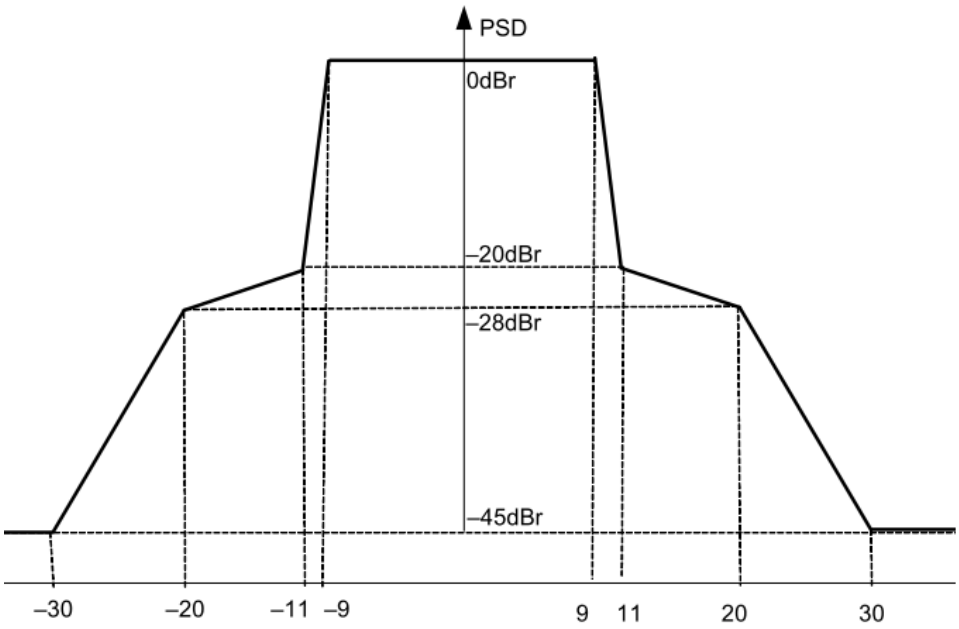

Рисунок 1.5 – Обвідна спектру випромінювання передавача

На відміну від стандартів 802.11 і 802.11b, навіть часткове перекриття цієї смуги може призвести до помилок передачі. На щастя в діапазоні 5 ГГц відстань між каналами становить ці самі 20 МГц.

Стандарт 802.11g не став проривом в плані швидкості передачі даних. Фактично цей стандарт став компіляцією 802.11a і 802.11b в діапазоні 2,4 ГГц: в ньому підтримувалися швидкості обох стандартів.

Серйозне збільшення швидкості сталося в стандарті 802.11n (в обох діапазонах 2,4 і 5 ГГц): до 72 Мбіт/с за рахунок зменшення захисних інтервалів між переданими символами. Крім того, для збільшення пропускної здатності можна було об’єднати два канали по 20 МГц і отримати 150 Мбіт/с. Однак це не найкращий спосіб збільшення швидкості: в діапазоні 2,4 МГц може поміститися всього один додатковий канал в 40МГц. Ще одним способом підвищення швидкості стала технологія MIMO: використання декількох приймачів, що працюють на одній і тій же частоті. Поділ каналів відбувається за рахунок просторового рознесення антен і математичних операцій над сигналом, прийнятим на різні антени: він буде відрізнятися в силу багатопроменевого поширення радіохвиль. Стандарт 802.11n підтримує MIMO 4x4:4 (чотири незалежних канали) і забезпечує швидкість до 600 Мбіт/с.

Однак дана технологія вимагає високої якості виготовлення радіо частини пристроїв. Крім того, дані швидкості принципово не реалізовуються на мобільних терміналах (основної цільової групи стандарту Wi-Fi): наявність 4-х антен на достатньому рознесенні не може бути реалізовано у малогабаритних пристроях як з міркувань відсутності місця, так і з-за відсутності достатньої енергії.

В більшості випадків швидкість 600 Мбіт/с є не більше, ніж маркетинговим прийомом і реалізовується на практиці, так як фактично її можна досягти тільки між стаціонарними точками доступу, встановленими в межах однієї кімнати при хорошому співвідношенні сигнал/шум.

Наступний крок у швидкості передачі був виконаний стандартом 802.11 ac: максимальна швидкість, передбачена стандартом, становить до 6,93 Гбіт/с, однак фактично така швидкість ще не досягнуто ні на одному обладнанні, представленому на ринку. Збільшення швидкості досягнуто за рахунок збільшення смуги пропускання до 80 і навіть до 160 МГц. Така смуга не може бути надана в діапазоні 2,4 ГГц, тому стандарт 802.11ac функціонує тільки в діапазоні 5 ГГц. Ще один фактор збільшення швидкості збільшення глибини модуляції до 256 рівнів на один символ. На жаль, така глибина модуляції може бути отримана тільки поблизу точки із-за підвищених вимог до співвідношення сигнал/шум. Зазначені поліпшення дозволили домогтися збільшення швидкості до 867 Мбіт/с. Решта збільшення отримано за рахунок раніше згаданих потоків MIMO 8x8:8. 867x8=6,93 Гбіт/с. Технологія MIMO була вдосконалена: вперше в стандарті Wi-Fi інформація в одній мережі може передаватися двом абонентам одночасно з використанням різних просторових потоків.

Таблиця 1.1 – Характеристика стандартів мережі Wi-Fi

Параметр	802.11b	802.11a	802.11g	802.11n	802.11ac
Макс. Швидкість	22	54	54	600	6930
Розширення спектра	DSSS	OFDM	DSSS/OFDM	OFDM	OFDM

Продовження таблиці 1.1

Збільшення швидкості завадостійкого коду	+	+	=	=	=
Збільшення глибини модуляції	+	+	=	=	+
Зменшення захисного інтервалу	-	-	-	+	=
Збільшення смуги	-	-	-	+	+
Просторові канали	-	-	-	+	+

У таблиці перераховані основні способи збільшення пропускної здатності « " - " – метод не застосуємо, » "+ " – швидкість була збільшена за рахунок даного фактора, " = " – даний фактор залишився без змін.

Ресурси зменшення надлишковості вже вичерпані: максимальна швидкість завадостійкого коду 5/6 була досягнута в стандарті 802.11a і з тих пір не збільшувалася. Збільшення глибини модуляції теоретично можливо, але наступною сходинкою є 1024QAM, яка є дуже вимогливою до співвідношення сигнал/шум, що гранично знизить радіус дії точки доступу на високих швидкостях. При цьому зростуть вимоги до виконання апаратної частини приймачів. Зменшення міжсимвольного захисного інтервалу також навряд чи буде напрямком вдосконалення швидкості – його зменшення загрожує збільшенням помилок, викликаних міжсимвольною інтерференцією. Збільшення смуги каналу понад 160 МГц так само навряд чи можливо, так як можливості по організації непересічних стільників будуть сильно обмежені. Ще менш реальним виглядає збільшення кількості MIMO-каналів: навіть два канала є проблемою для мобільних пристроїв (через енергоспоживання і габарити).

З перерахованих методів збільшення швидкості передачі, велика частина в якості розплати за своє застосування забирає корисна площа покриття: знижується пропускна здатність хвиль (перехід від 2,4 до 5 ГГц) і підвищуються вимоги до співвідношення сигнал шум (збільшення глибини модуляції, підвищення швидкості коду). Тому у своєму розвитку мережі

Wi-Fi постійно прагнуть до зменшення площі, що обслуговується однією точкою на користь швидкості передачі даних.

В якості доступних напрямків вдосконалення можуть використовуватися: динамічний розподіл OFDM піднесучих між абонентами в широких каналах, вдосконалення алгоритму доступу до середовища, спрямоване на зменшення службового трафіку і використання технік компенсації перешкод.

Взагалі тенденція зменшення зон обслуговування, схоже, є основним трендом в сучасних безпроводових комунікаціях. Деякі фахівці вважають, що стандарт LTE досяг піку своєї пропускної здатності та не зможе далі розвиватися з фундаментальних причин, пов'язаних з обмеженістю частотного ресурсу [2].

1.2 Роумінг в мережах стандарту IEEE 802.11

Коли мова заходить про роумінг, під цим поняттям зазвичай ховається два різних процеси. У світі стільникових мереж, який прийшов до нас раніше, під роумінгом мається на увазі здатність працювати в «чужій» мережі, а зовсім не безшовна міграція між базовими станціями (handover). Непомітне переміщення між БС мережі настільки природно, що про нього взагалі мало згадують.

У світі Wi–Fi справи йдуть інакше, і під роумінгом зазвичай мають на увазі непомітне для користувача переміщення між точками доступу однієї мережі – BSS transition, хоча повсюдне введення SMS-авторизації в найближчому майбутньому має підштовхнути операторів до впровадження стандарту роумінгу між чужими мережами Wi–Fi в стилі стільникової інфраструктури і на базі її ідентифікації.

В стільникових мережах перемикання абонента на іншу БС ініціює контролер мережі на основі інформаційних повідомлень від клієнта, оцінюючи сигнал на клієнті від сусідніх баз, Wi–Fi рішення про переключення клієнт

завжди приймає сам – база може лише підказати, як це зробити швидше. Зате в Wi–Fi є безліч стандартів, які цілком успішно дозволяють укласти процес зміни точки доступу в 50 мс і зберегти абоненту голосовий дзвінок поверх IP, а також не стандартизованих розробок кожного виробника, які можуть як допомогти, так і погіршити і без того сумний процес.

OKC (Opportunistic Key Caching). В процесі автентифікації 802.1x точка доступу зберігає ключ pairwise master key (PMK) для кожного клієнта, ідея полягала у тому щоб цей ключ через контролер передавався сусіднім точкам – за рахунок чого виключалося нове звернення до RADIUS і спрощувався обмін, значно знижувався час перемикання на нову точку.

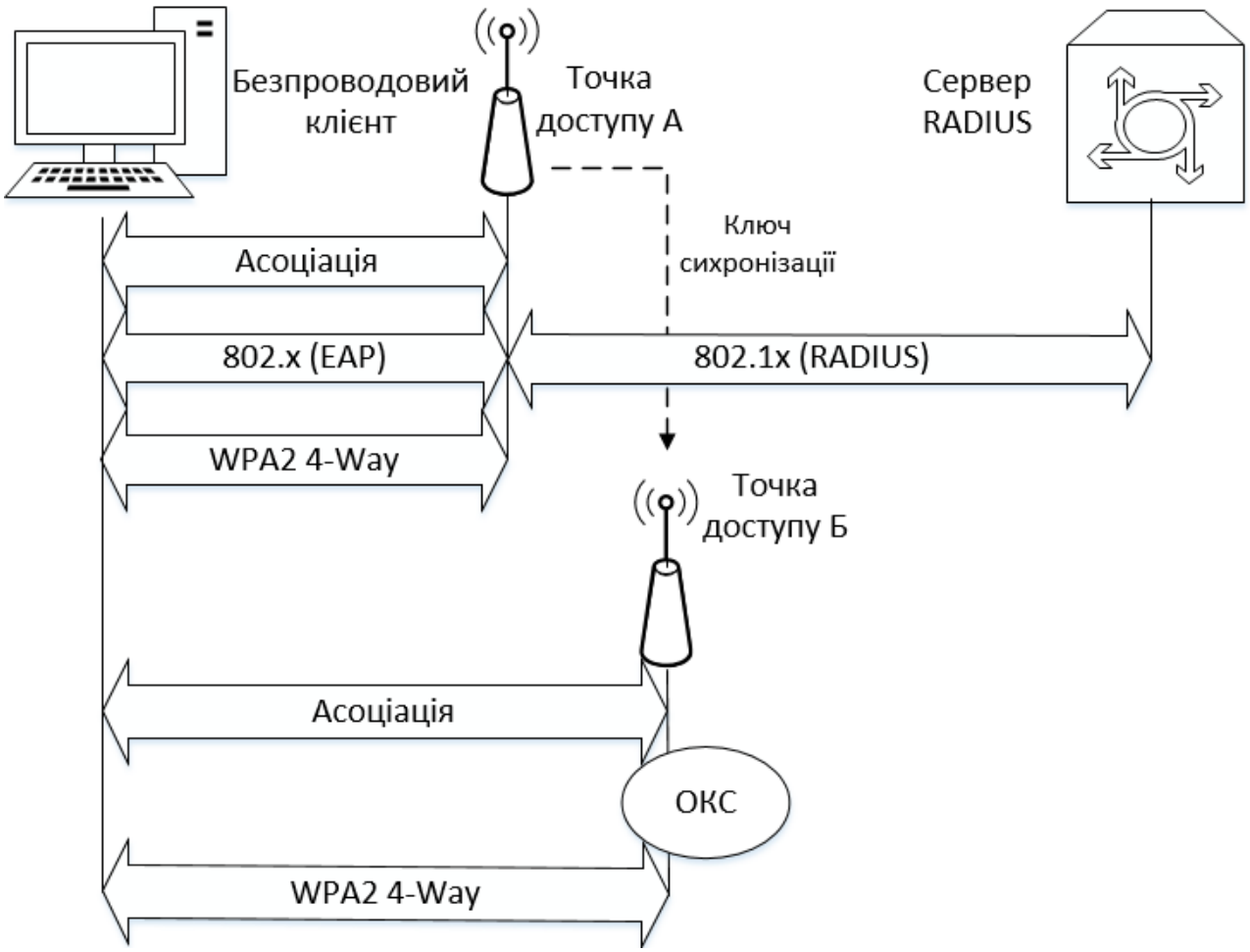

Рисунок 1.6 – Технологія ОКС

За час існування безпроводових мереж IEEE 802.11 процес взаємодії абонента з мережею зазнав суттєвих змін і його продовжують удосконалювати. Далі коротко проаналізовано найбільш важливі удосконалення процесу взаємодії.

Специфікація 802.11 i. Поправка 2004 року, внесена в стандарт в 2007, націлена на безпеку і описує автентифікацію і шифрування (WPA2). Процедура обміну ключами і взаємодія із зовнішніми ресурсами (RADIUS) разом сильно уповільнюють перемикання клієнта між ТД. Описаний перший принцип швидкого перепідключення – зберігання ключа PMK, правда, тільки для тих точок де клієнт один раз вже пройшов повну процедуру – тобто швидке повернення в мережу.

Специфікація 802.11 k. Точка доступу прапором вказує в Beacon підтримку опції, при запиті з боку клієнта відправляє йому список сусідніх точок, клієнт не витрачає час на сканування всіх доступних каналів і відразу переходить на потрібний і вибирає нову точку. Економиться батарейка, в High-Load також поліпшується загальний стан ефіру. Разом з 802.11v може зробити життя клієнтів досить комфортним, щоб не думати про інші технології – якщо звичайно вам не важливий VoIP і магія 50 мс для WPA2-Enterprise. Без підтримки з боку клієнта марна.

Специфікація 802.11v. Wireless Network Management (WNM) поправки опубліковані в 2011 році і в 2012 ввійшли в стандарт, велика кількість опцій. Основне призначення – ефективне управління безпроводовим середовищем – обмін даними про середовище між станціями, енергозбереження клієнта, покращення процесу роумінгу і балансування – клієнту повідомлення надсилається з відповідними ТД, що адресує проблеми перевантаження точок (Load-Balancing) і "прилиплих" клієнтів зі слабким сигналом та деякі інші функції. Assisted Power Saving встановлює максимальний тайм-аут для клієнта, не вимагаючи від нього частих повідомлень keep-alive, Direct Milticast Service дозволяє отримувати мультикаст-кадри на швидкості підключення клієнта, а не швидкості стільника – що звільняє ефір і зберігає батарею (до роумінгу дані

функції не належать). А ось до BSS Transition дуже навіть належить – в її рамках існує 3 типи повідомлень, це запит від клієнта на зазначення відповідних точок, і два повідомлення від точки – Load Balancing Request у разі якщо точка перевантажена, і просить клієнта перейти на іншу і Optimized Roaming Request якщо параметри RSSI і Data Rate не задовольняють мінімальним вимогам ТД. Важливо відзначити, що це рекомендаційні повідомлення, і дії залишаються на розсуд клієнта. Примусове відключення можливе тільки в рамках технологій Band/Load Steering/Balancing, і може бути некоректно відпрацьовано клієнтом, або зовсім ігнорується (його відключають кадрами Disassociate).

Спільне використання 802.11k/v дає хороший результат не створюючи проблем в роботі різних пристроїв. Далі вже йде важка артилерія – вона радикально вирішує основну проблему, але може викликати побічні дії – це 802.11r.

Специфікація 802.11r/FT. Fast Roaming/Fast BSS Transition – 802.11r обов'язкове для клієнта при використанні на точці, тобто ті хто її не підтримує, не можуть підключитися – це прапор в керівних кадрах і змінений механізм обміну ключами, якщо абонент старий і не знає про його існування, у нього проблема (на нових пристроях навіть за відсутності підтримки функції іноді додають розуміння даного прапора, хоча за стандартом потрібно повністю реалізувати протокол).

Fast BSS Transition працює з мережами RSNA (Robust Security Network Association – WPA2) і повністю відкритими мережами. Для WPA2-PSK втрачається сенс швидкого роумінгу, тому що клієнт і точка все одно обмінюються 4 пакетами, прискорювати тут нічого. В розрахунках не враховується час на пошук потрібної точки, а для діапазону 5 ГГц воно може бути неабияким – необхідно відсканувати 16 каналів і знайти відповідну ТД, тому загальна стратегія як раз полягає у спільному використанні протоколів k/v і r.

Якщо ви використовуєте для авторизації RADIUS і хочете дуже швидкий

роумінг – вибору у вас немає, тільки 802.11r.

Крім самого роумінгу в 802.11r потенційно є можливість опитувати точку про наявність необхідних клієнту ресурсів і резервувати їх (QoS). Відповідно, існує два підвиди протоколів – FT Protocol і FT Resource Request Protocol. Взаємодія між клієнтом і точками може відбуватися як безпосередньо через повітря (Over-the-Air), так і через якусь точку та контролери (Over-the-DS) – другий спосіб трохи довше. Запит QoS від точки на клієнтах поки практично ніде не реалізований і не використовується. айважливіший елемент кадру – MDE, Mobility Domain Element, він необхідний для успішного роумінгу, який можливий тільки в межах одного домену [3].

1.3 Аналіз особливостей використання локальних безпроводових мереж стандарту 802.11

Для аналізу мережі Wi-Fi створимо завдання, сенс якого зводиться до організації мережі Wi-Fi для доступу в Інтернет на об’єкті, призначеному для проведення великих громадських заходів. Площа об’єкта 4000 м2, число активних користувачів – до 2000 осіб (клієнтських пристроїв). Швидкість доступу: бажано 10 Мбіт/с при гарантованому 1 Мбіт/с кожному користувачеві.

Виходячи з того, що більшість смартфонів підтримують реалізацію стандарту 802.11n з одним просторовим потоком (1ss). Максимальна ефективна швидкість передачі даних у мережі IEEE 802.11n при використанні каналу 20 МГц (HT20), одного потоку (1ss) і схеми кодування/модуляції MCS7 – 35 Мбіт/с. Відповідно, для забезпечення необхідної пропускної здатності (1-10 Мбіт/с) на однин кінцевий пристрій число абонентів на одному радіоінтерфейсі точки доступу не має перевищувати 30. Згідно з теоретичними розрахунками, для забезпечення одночасної роботи 2000 клієнтських пристроїв на території 4000м2 з гарантованою мінімальною швидкістю 1 Мбіт/с потрібно встановити не менше 67 точок доступу.

Переважна більшість клієнтів (85%) можуть використовувати тільки один просторовий потік, причому більша їх частина (70%) здатні працювати тільки в діапазоні 2,4 ГГц. При цьому, що 5% користувачів володіють топовими ноутбуками, що підтримують три просторові потоки і обидва діапазони Wi-Fi. За стандартом 802.11n при використанні зазначеного числа потоків теоретично швидкість може доходити до 450 Мбіт/с.

Таблиця 1.2 – Розподіл типів клієнтів

Технологія	Частина клієнтів, %	Тип клієнтів
802.11n 1x1:1 (тільки 2,4 ГГц)	70	Старі моделі смартфонів і планшетів
802.11n 1x1:1 (два діапазона)	15	Нові сматрфони і планшети
802.11n 2x2:2 (тільки 2,4 ГГц)	5	Ультрабуки
802.11n 2x2:2 (два діапазона)	5	Ноутбуки середнього рівня, нові планшети
802.11n 3x3:3 (два діапазона)	5	Топові ноутбуки

Варіант з найменшим числом пристроїв передбачає установку всього чотирьох точок доступу ZoneFlex R700 з всеспрямованими антенами. Звичайно, чотири точки не здатні забезпечити одночасну роботу всіх 2000 клієнтів, але з 800 пристроями цілком впораються. По 200-250 асоційованих клієнтів на точку, при використанні Ruckus ZoneFlex R700 на конференції. У трьох інших варіантах пропонується точки доступу з спрямованими антенами.

Таблиця 1.3 – Варіанти вирішення завдання

Назва/Вар	Вар 1	Вар 2	Вар 3	Вар 4
Продуктивність на клієнта, Мбіт/с	0.5	0.5	1	1
Кіл-сть підключених клієнтів	800	2000	2000	2000
Кіл-сть одночасних підключених клієнтів	160	800	800	1000
Кіл-сть необхідних точок	4	17	30	57
Тип точки доступу	ZoneFlex R700	ZoneFlex T301S	ZoneFlex T301N	ZoneFlex T301N
Кіл-сть клієнтів на ТД при 2,4 ГГц	170	100	57	30
Кіл-сть клієнтів на ТД при 5 ГГц	30	18	10	5
Вимоги до каналу в інтернеті, Мбіт/с	80	400	800	1000
Контролері	ZoneDirector 1200	ZoneDirector 1200	ZoneDirector 1200	ZoneDirector 1200
Ліцензії для точок доступу	В комлекті	11	24	51

Компанія Aruba представила графік падіння швидкості, доступної кожному користувачеві, при зростанні числа підключень до точки доступу (рис. 1.7). Він був побудований на основі результатів тестування роботи мережі Wi-Fi при різному співвідношенні числа клієнтів 802.11n HT20 і клієнтів 802.11a. (В якості клієнтів в тесті використовувалися 50 ноутбуків і нетбуків різних виробників, з різними ОС і типами безпроводових адаптерів.) З графіка видно,

що навіть при самому сприятливому розкладі (100% клієнтів використовують 802.11n HT20) з урахуванням сформульованих замовником вимог одна ТД зможе обслуговувати максимум 50 користувачів. Відповідно, для вирішення завдання буде потрібно мінімум 40 ТД.

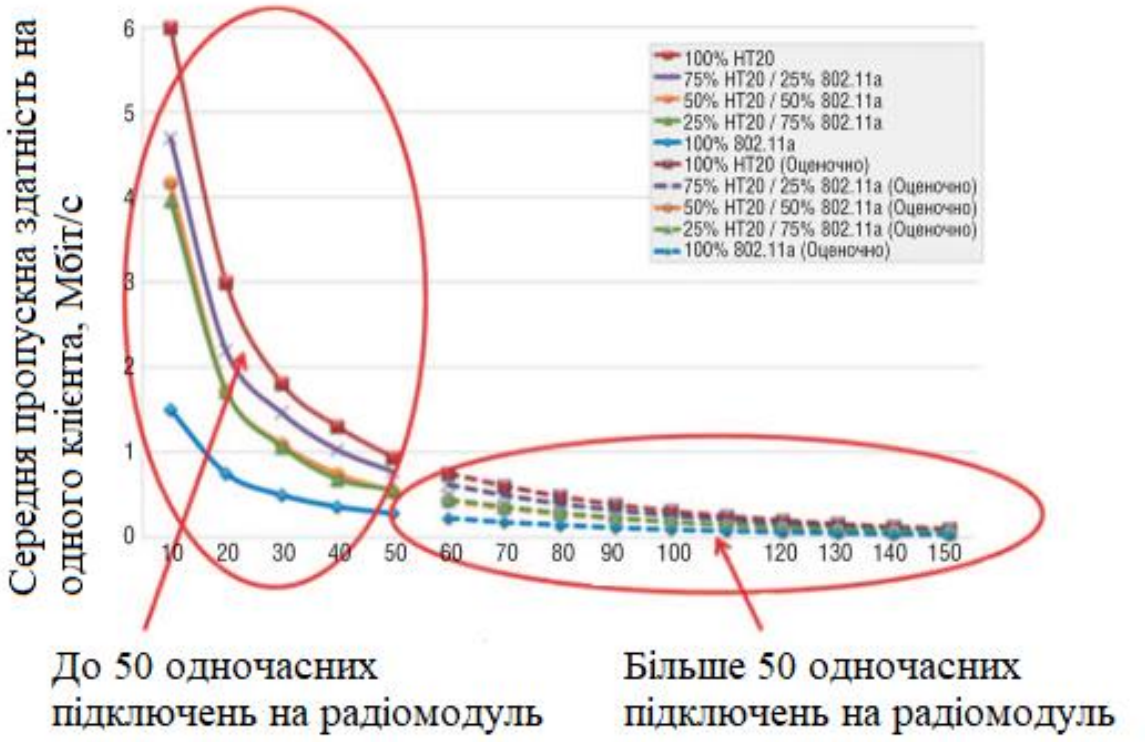

Рисунок 1.7 – Падіння швидкості, доступної кожному користувачеві, при зростанні числа підключень до точки доступу.

У сценаріях Wi-Fi високої щільності часто правильніше використовувати антени з вузькою діаграмою спрямованості. Тому був зроблений розрахунок з використанням точок доступу Huawei AP8130DN з спрямованими антенами. Правда, це зовнішні ТД, що істотно підвищує вартість рішення. В цьому випадку достатньо 28 точок доступу. Але тоді швидкість буде забезпечена тільки 840 одночасним користувачам при загальній кількості асоційованих користувачів, що дорівнює 2000.

Всі експерти радять по можливості задіяти більш вільний і ресурсномісткий діапазон 5 ГГц, а запропоновані рішення передбачають примусове підключення клієнтів, що підтримують діапазон 5 ГГц, до

відповідних точок доступу. Фахівці Aruba рекомендують використовувати пікостільники, по можливості зводячи до мінімуму кількість клієнтів на одній точці доступу (з урахуванням вимоги до пропускної здатності), а також задіяти систему управління частотами для зниження впливу один на одного сусідніх точок доступу.

Для ефективного використання радіоспектру у відкритих просторах з великою щільністю абонентів слід обмежити зони дії точок доступу за рахунок застосування спеціалізованих антен малого радіусу дії. Крім того, потрібно відключити низькі канальні швидкості і обробку пакетів абонентів з низьким рівнем сигналу (RX-SOP), а для безшовного роумінгу – забезпечити 20-відсоткове перекриття зон обслуговування сусідніх точок.

Серед заходів, спрямованих на зниження інтерференції, існує здатність (контролера) автоматично управляти потужністю кожної з точок доступу.

При установці десятки точок з всеспрямованими антенами рівень інтерференції в діапазоні 2,4 ГГц може становити близько 50%, тобто половину часу ТД не зможуть передавати дані із-за великої кількості колізій. Це викликано тим, що в зазначеному діапазоні є обмежене число неперекриваючих каналів, точніше всього три – 1, 6, 11, і при високій щільності установки точок доступу, що працюють на одному каналі і знаходяться в зоні радіодоступу, будуть заважати один одному. Зниження потужності передавача призводить до зменшення рівня сигналу на антені клієнта, зниження рівня модуляції і, як результат, падіння швидкості передачі, що в кінцевому підсумку обертається зменшенням загальної ємності безпроводової мережі.

Компанія Ruckus пропонує застосовувати в точках доступу активні антенні решітки, здатні формувати діаграму спрямованості в потрібному напрямку (в бік знаходження клієнта). Це дозволяє задіяти передавач точки доступу на повну потужність, щоб обмінюватися даними з клієнтом на максимально можливих швидкостях. В результаті вдається домогтися більш високої ємності безпроводової мережі (в порівнянні з використанням звичайних точок доступу з традиційними всеспрямованими антенами).

Розроблені Ruckus антенні решітки BeamFlex забезпечують формування точкою доступу до декількох тисяч унікальних діаграм спрямованості для кожного окремого клієнта і навіть для кожного пакету даних у відповідності з особливостями радіосередовища в даний момент часу в даному місці. За рахунок цього значно, до 8 разів, підвищується рівень корисного сигналу на антені клієнта, що дозволяє йому працювати при більш високій модуляції і отримувати дані з більш високою швидкістю. Так як ТД фокусує радіосигнал в певному напрямку, вона має менший негативний вплив на сусідні точки доступу, а ємність безпроводової мережі істотно підвищується.

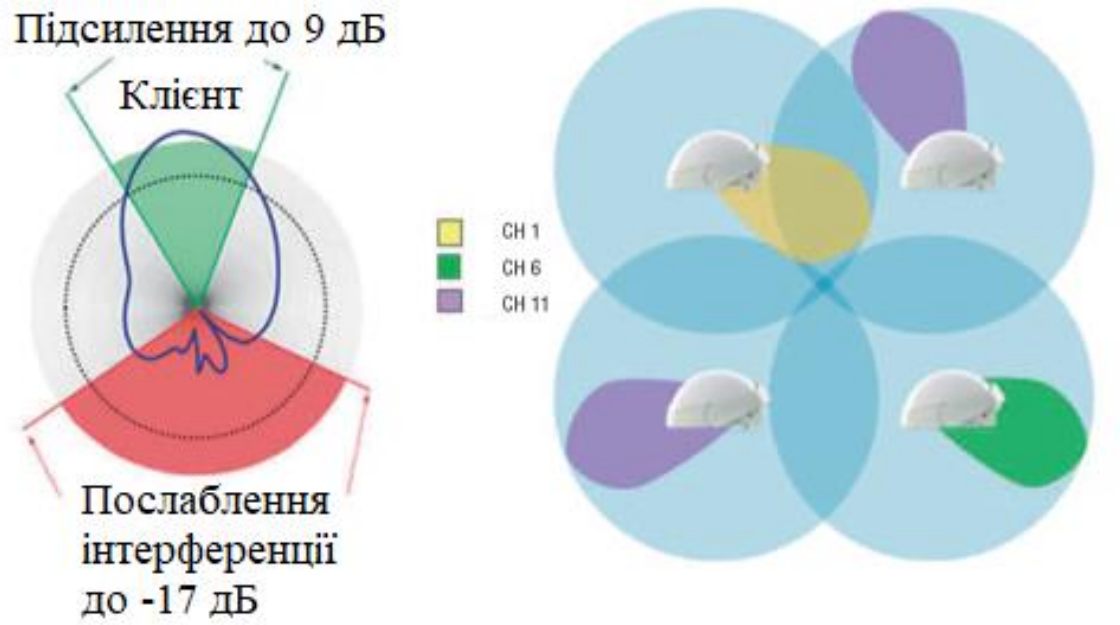

Рисунок 1.8 – Діаграми спрямованості антенних решіток BeamFlex

Чи можна вирішити завдання замовника, встановивши всього один пристрій? Теоретично – так. Такий варіант згадали в своєму проекті фахівці компанії «Тритфейс», і він реалізований за допомогою унікального масиву Xirrus XR-7630, який містить 16 точок доступу з секторними антенами і вбудованим контролером (рис. 1.9). Загальна пропускна здатність інтерфейсів Wi-Fi цього пристрою становить 7,2 Гбіт/с, що при наявності 2000 клієнтів дає 3,6 Мбіт/с на користувача. Однак, як відзначають експерти «Тритфейс», в даному разі досягнення поставлених цілей можливо тільки при застосуванні

високопродуктивних клієнтських адаптерів 802.11ac с MIMO 3x3, що формально відповідає умовам завдання і досяжна в ідеальних умовах, але на поточний момент дещо відірвано від реальності.

Як варіант, що відповідає реальному стану парку клієнтських пристроїв, вони запропонували проект, що передбачає інсталяцію чотирьох масивів Xirrus XR-7630. На їхню думку, в даний момент на ринку переважають кінцеві пристрої 802.11n SISO і MIMO 2x2. Крім того, з'являється все більше дводіапазонних пристроїв, причому частка клієнтів, здатних працювати в діапазоні 5 ГГц, вже перевищує 50%.

Рисунок 1.9 – Масив Xirrus XR-7630 містить 16 точок доступу з секторними антенами і вбудованим контролером

Рисунок 1.10 – Комплект швидкого розгортання Xirrus

Як стверджують в «Тритфейс», використання масивів дозволяє істотно заощадити на кабельній інфраструктурі – в даному випадку достатньо організувати підключення до мережі тільки чотирьох пристроїв, а не кілька десятків, як в інших проектах. Крім того, очевидні переваги такого рішення з точки зору швидкості інсталяції.

Облік і контроль

Завдяки функції безперервного DPI-аналізу трафіку, ідентифікація сервісів і додатків здійснюється безпосередньо на масиві. За допомогою заданих правил можна обмежувати за швидкістю/пріоритетом той чи інший сервіс, а також повністю його блокувати.

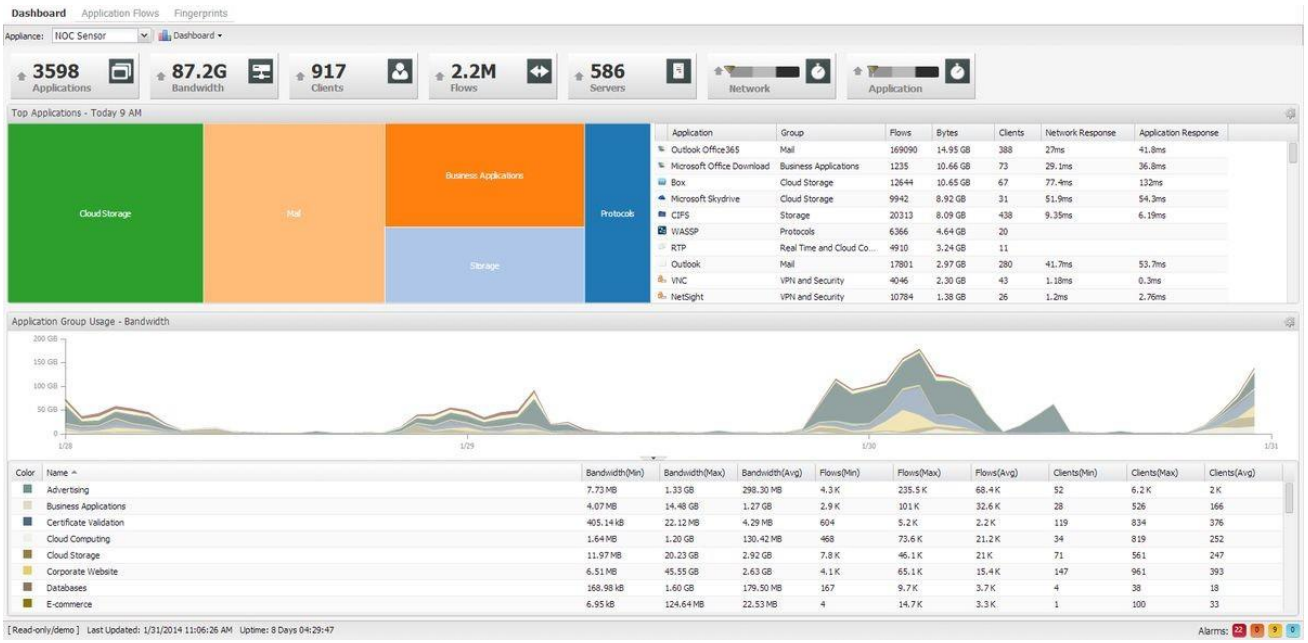

Рисунок 1.11 – Скріншот результатів вимірювання параметрів Wi-Fi мережі засобами програми Purview

Система Purview – програмно-апаратний комплекс, який здійснює сигнатурний аналіз трафіку і дозволяє отримувати інформацію про склад працюючих в мережі додатків. Система розбирає загальний потік трафіку на інформаційні потоки додатків, виокремлює з кожного потоку інформативну з точки зору ідентифікації додатка частину (перші 20-30 пакетів) і піддає цю інформативну частину подальшому аналізу. Крім інформації про склад трафіку, Purview оцінює стан мережі відносно часу відгуку додатків, що дозволяє мережному адміністратору оперативно та цілеспрямовано реагувати на виникаючі в мережі несправності і відслідковувати якість сервісу.

Для забезпечення безпеки і захисту від зовнішніх вторгнень Huawei запропонувала міжмережевий екран USG6360, який дозволяє, зокрема, здійснювати глибокий аналіз трафіку і розпізнавати понад 6000 різних типів додатків і мережевих сервісів (можна обмежити закачування торрентів, обмежити смугу для певного сервісу тощо). Для централізованого контролю і управління терміналами, користувачами, правилами доступу і політиками

безпеки компанія Huawei пропонує програмно-апаратний комплекс Agile Controller, який одночасно є і SDN-контролером [4].

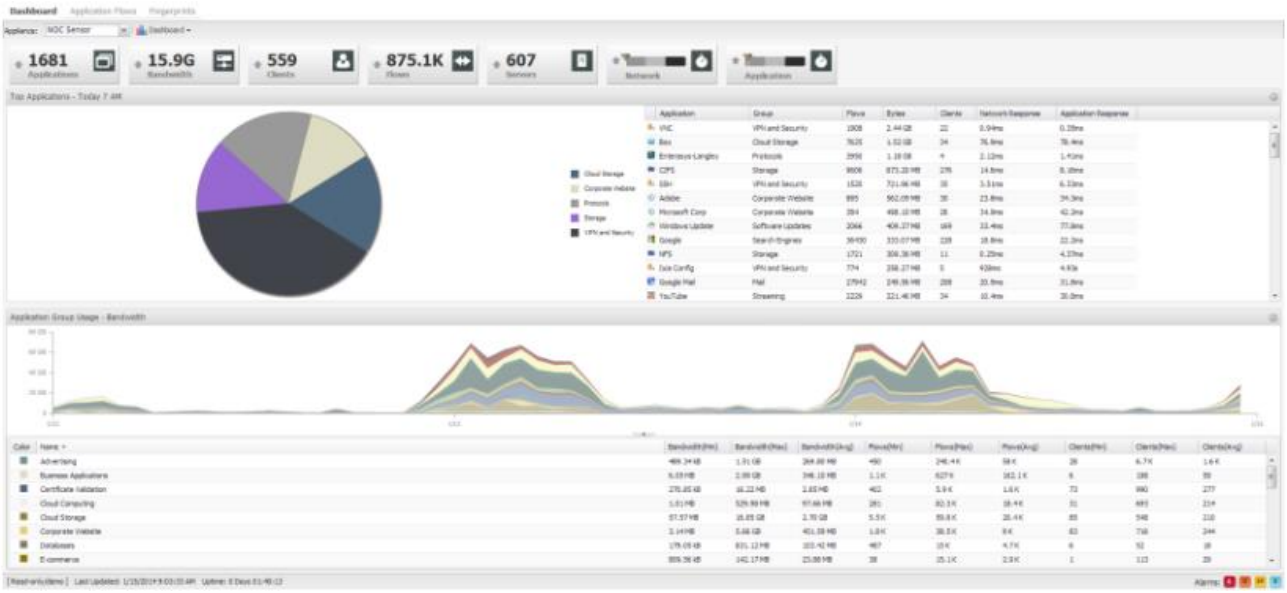

Рисунок 1.12 – Результати сигнатурного аналізу та визначення використаних в мережі додатків засобами програми Purview

1.4 Рекомендації щодо організації мереж стандарту IEEE 802.11 в місцях великого скупчення людей

Перш за все необхідно відзначити, що сучасні підходи проектування мереж з високою щільністю ґрунтуються на розумінні того, що основний користувач в такому сценарії це людина з мобільним пристроєм. Загальна кількість присутніх людей в таких місцях дуже велика, тому кількість потенційних користувачів мережі Wi-Fi також може бути великою.

Ще не так давно до мережі Wi-Fi ставились з недовірою, оскільки її безпека порівнюючи з прийнятою в мережі 3G вважалася слабкою за ступенем захищеності та прозорості процесу аутентифікації абонентів. Однак в даний час більшість операторів мереж мобільного зв’язку вважає, що з реалізацією технологій 802.1x, 802.11i, 802.11u і HotSpot 2.0 ступінь захищеності і зручність використання Wi-Fi стали відповідати рівню 3G і LTE.

Ось які проблеми стоять перед проектувальниками безпроводових мереж високої щільності:

– Інтерференція від інших Wi-Fi мереж.

– Інтерференція від інших пристроїв, що працюють в цьому діапазоні.

– Міжканальна інтерференція внаслідок близького розташування точок доступу.

– Складність розміщення та інсталяції обладнання.

– Зниження продуктивності мережі через клієнтів, що використовують стандарт IEEE 802.11b.

– Зниження швидкості передачі через неправильний розподіл клієнтів по діапазонах (використання діапазону 2.4 ГГц, коли можна використовувати діапазон 5 ГГц).

– «Залипання» клієнтів, коли пристрій залишається підключеним до точки доступу навіть коли клієнт перемістився на інший кінець об'єкта тощо.

Wi-Fi на стадіонах: технологія високої щільності

Найбільші спортивні майданчики світу вміщують величезну кількість глядачів. Глядачі будь-яких спортивних подій, звичайно ж, відразу хочуть поділитися своїми емоціями і враженнями з друзями в соціальних мережах. І, крім текстових повідомлень, відвідувачі у величезній кількості викладають фото, відео, а іноді навіть ведуть прямі трансляції. Мережі 3G і 4G не завжди можуть впоратися з цим завданням, і тоді їм на допомогу приходить Wi-Fi, що надає глядачам безпроводовий доступ в інтернет на території всього спортивного об'єкта. Для стадіонів така послуга – скоріше данина прогресу, показник відповідності сучасним технологіям, ніж необхідний елемент обслуговування, як в ресторанах і кафе. Адже розгорнути безпроводову мережу в умовах високої щільності клієнтів навіть на стадіоні в 10 тисяч осіб – складне і трудомістке завдання, не кажучи вже про фінансову складову питання. І все-таки вдалих прикладів проектування Wi-Fi-мереж на стадіонах достатньо.

Звичайно, класична схема, де використовуються точки доступу з всеспрямованими антенами, розраховані на 20-30 клієнтів, тут не працює. На

стадіоні щільність користувачів становить приблизно 2-3 клієнта на квадратний метр, тобто точка доступу може просто не впоратися з навантаженням. З іншого боку, при установці занадто великої кількості точок доступу або при збільшенні їх потужності не уникнути інтерференційних перешкод. Також слід пам'ятати про пропускну здатність обладнання - чим більше радіус дії антени, тим більша кількість користувачів може підключитися до точки доступу. Відповідно, пропускна здатність, розрахована на одного клієнта, знизиться. При цьому діапазон 2.4 ГГц обмежений лише трьома непересічними каналами, в той час як в діапазоні 5 ГГц їх 11. Однак далеко не всі пристрої підтримують 5 ГГц, а значить мережа повинна бути розрахована на обидва діапазони. Збільшити смугу пропускання може використання точок доступу, що підтримують стандарт IEEE 802.11ac. Він дозволяє не тільки збільшити кількість клієнтів в стільнику, але і забезпечити роботу високоємних додатків. Також для розвантаження мережі може бути використана технологія Band Select, яка примусово переводить клієнтів з двома діапазонами в 5 ГГц. Крім цього необхідно зменшення радіусу дії точок доступу для створення невеликих зон обслуговування. Для цього використовуються антени з вузькою діаграмою спрямованості, зменшується потужність передавача, відключаються низькі канальні швидкості (при відсутності клієнтів IEEE 802.11b) і відключається обробка пакетів абонентів з низьким рівнем сигналу (наприклад, технологія Cisco RX-SOP). Інтерференція від інших мереж і пристроїв також скорочується шляхом зменшення потужності і радіусу дії точок доступу.

Потужність точок доступу бажано виставляти відповідно до максимальної потужністю самого малопотужного пристрою в мережі для того, щоб уникнути утворення несиметричних каналів і провалів в покритті мережі. Якщо зону покриття точки доступу потрібно збільшити, то слід збільшити потужність антени, а не передавача.

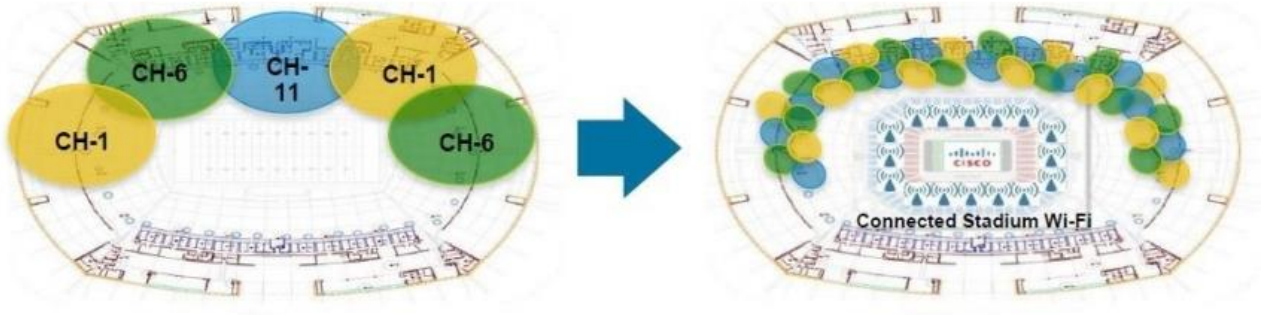

Рисунок 1.13 – Поліпшення зони охоплення і пропускної спроможності за допомогою Cisco Connected Stadium Wi-Fi

Ще один важливий момент – це кількість використовуваних SSID. На стадіонах часто існує сегментація мережі з різними SSID – для преси, для коментаторської будки, для VIP-гостей тощо. З одного боку, це дуже зручно, а з іншого, виникають певні складності. Справа в тому, що мережа посилає керуючі кадри з кожного SSID, тому радіоефір Wi-Fi-мережі високої щільності виявляється частково зайнятим керуючим трафіком. Для того щоб уникнути такої ситуації, використовують мінімальну кількість SSID. В ідеалі він повинен бути один.

Що стосується обладнання, то найбільші виробники, такі як Cisco Systems, Aruba Networks, Ruckus, Extreme Networks, Huawei та інші компанії пропонують комплексні рішення. До таких можна віднести, наприклад, Cisco Connected Stadium Wi-Fi. Основні компоненти подібної системи-контролери (основний і резервний) для централізованого управління, точки доступу і антени. Кожна точка доступу розрахована приблизно на 250-500 користувачів. Антени, як і точки доступу, повинні підтримувати два діапазона – 2.4 и 5 ГГц і технологію MIMO. Бажано, щоб користувальницькі пристрої і антени знаходилися в зоні прямої видимості, тобто антени повинні бути встановлені на стінах стадіону або на даху з внутрішньої сторони [5].

Безпроводова мережа, побудована за традиційним дизайном, не впорається з поставленими завданнями. В результаті вийшли б великі втрати

пакетів, велика кількість ретрансмітерів, і, як наслідок – вкрай низька швидкість передачі даних, нестабільна робота сервісів.

Зменшення зон дії точок доступу досягається за рахунок:

— застосування спеціалізованих вузькоспрямованих антен;

— відключення низьких канальних швидкостей (до 12 Мбіт/с);

— відключення обробки пакетів абонентів з низьким рівнем сигналу (RX-SOP);

— зниження потужності передавача;

Ще потрібно:

1. Захистити зону HD-покриття від паразитного сигналу Wi-Fi. Негативні явища на покриття глядацької зони чаші стадіону можу надати свої ж точки, розташовані в VIP-зонах, вестибюлях поблизу виходів на поле. Рецепт той же – контроль потужності і радіопокриття.

2. Скоротити утилізацію радіоканалу: не використовувати більше чотирьох SSID (в ідеалі використовувати один) в зорових зонах, тому що кожен SSID вимагає відправки окремого Beacon пакету і кожен широкомовний SSID відповідає на null probe request; боротися з клієнт-спровокованими перешкодами, запропонувавши глядачам підключитися до Wi-Fi мережі, тому що підключений пристрій починає відсилати probe request в рази рідше; максимально усунути із зони дії безпроводової мережі сторонні точки доступу і Ad Hoc пристрої як джерела інтерференції і генератори beacon, probe request, probe response пакетів і відмовитися від використання «суміжних» Wi-Fi мереж і використовувати єдину безпроводову мережу [6].

Планування в готелі. З точки зору розгортання безпроводової мережі типовий готель дещо складніше офісного open space або кав'ярні. Так, щільність підключення клієнтів тут не так висока, але на поширення сигналу впливають стіни, меблі, елементи інтер'єру, труби та інші інженерні споруди. При цьому для кінцевого результату (для надання якісної послуги постояльцям) вкрай важливо співвідношення рівнів сигналу і шуму в будь-якому місці готельного номера. Тому ще на етапі проектування мережі необхідно провести

повноцінне радіообстеження і радіопланування, що дозволяють визначити оптимальні точки розміщення обладнання.

Хороша точка доступу для готелів повинна бути дводіапазонною. Пристрій має забезпечувати балансування навантаження, у тому числі за рахунок функції Band Steering, що дозволяє перемикати в діапазон 5 ГГц клієнтів з підтримуючими його пристроями, звільняючи смугу в діапазоні 2,4 ГГц (для пристроїв, які не підтримують другий діапазон).

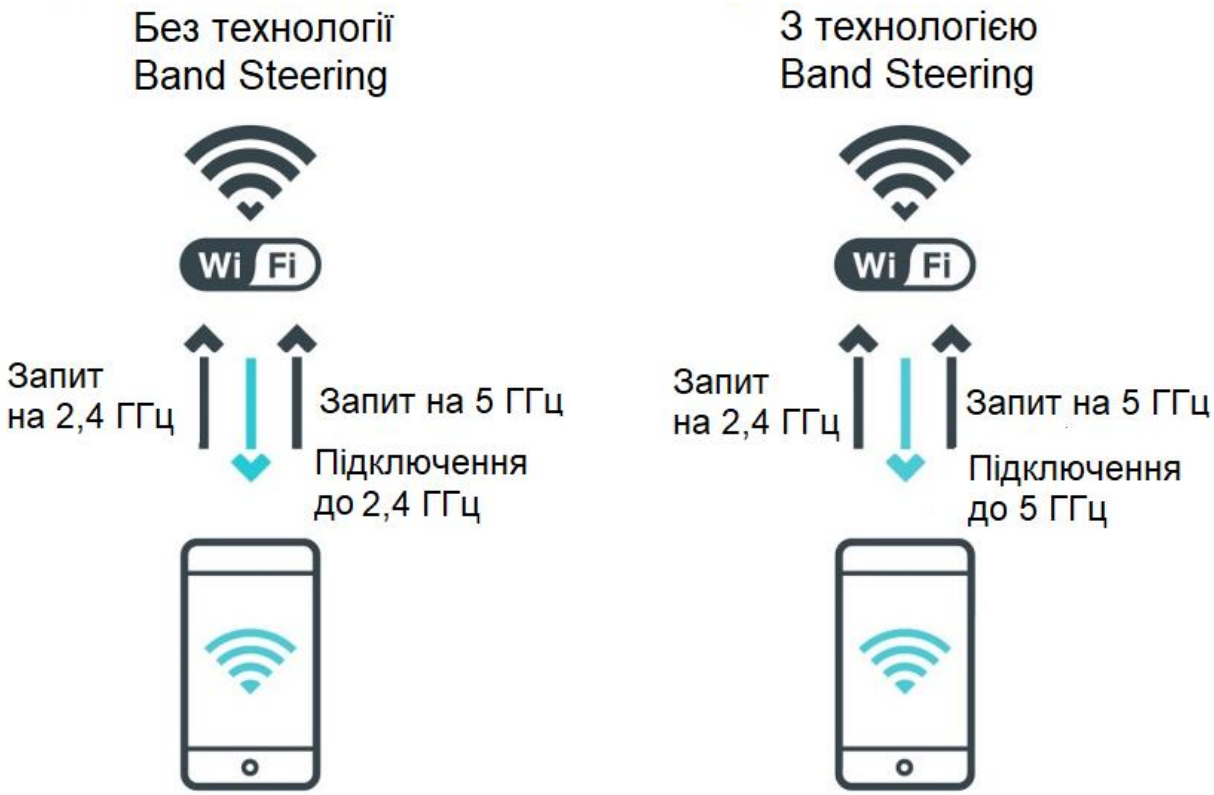

Рисунок 1.14 – Технологія Band Steering

У нових пристроях для безпроводового зв’язку для приміщень (тобто тих місць, де поширення сигналу утруднене перекриттями, меблями тощо) передбачена технологія Beamforming, яка змінює умови передачі сигналу в залежності від особливостей оточення. Пристрій визначає, за яким напрямом найбільші втрати сигналу, причому вирішуватися це завдання може як спільно з абонентським пристроєм, так і точкою доступу самостійно, в залежності від підтримуваних клієнтом стандартів.

Рисунок 1.15 – Приклад застосування технології Beamforming

Варто відзначити технологію, яка вже стала обов'язковою в мережах рівня Enterprise: Airtime Fairness, що забезпечує захист від «повільного клієнта», який тепер не зможе монополізувати ресурси точки доступу і не погіршить загальну продуктивність мережі [7].

Висновки до розділу

1. З перерахованих методів збільшення швидкості передачі, велика частина в якості розплати за своє застосування забирає корисна площа покриття: знижується пропускна здатність хвиль (перехід від 2,4 до 5 ГГц) і підвищуються вимоги до співвідношення сигнал шум (збільшення глибини модуляції, підвищення швидкості коду). Тому у своєму розвитку мережі Wi-Fi постійно прагнуть до зменшення площі, що обслуговується однією точкою на користь швидкості передачі даних.

Взагалі тенденція зменшення зон обслуговування, схоже, є основним трендом в сучасних безпроводових комунікаціях. Деякі фахівці вважають, що стандарт LTE досяг піку своєї пропускної здатності та не зможе далі

розвиватися з фундаментальних причин, пов’язаних з обмеженістю частотного ресурсу.

2. Під роумінгом розуміють здатність працювати в «чужій» мережі, а зовсім не безшовна міграція між базовими станціями (handover).

В стільникових мережах перемикання абонента на іншу БС ініціює контролер мережі на основі інформаційних повідомлень від клієнта, оцінюючи сигнал на клієнті від сусідніх баз, Wi–Fi рішення про переключення клієнт завжди приймає сам – база може лише підказати, як це зробити швидше. Зате в Wi–Fi є безліч стандартів, які цілком успішно дозволяють укласти процес зміни точки доступу в 50 мс і зберегти абоненту голосовий дзвінок поверх IP, а також не стандартизованих розробок кожного виробника, які можуть як допомогти, так і погіршити і без того сумний процес.

3. Виходячи з того, що більшість смартфонів підтримують реалізацію стандарту 802.11n з одним просторовим потоком (1ss). Максимальна ефективна швидкість передачі даних у мережі IEEE 802.11n при використанні каналу 20 МГц (HT20), одного потоку (1ss) і схеми кодування/модуляції MCS7 – 35 Мбіт/с.

У сценаріях Wi-Fi високої щільності часто правильніше використовувати антени з вузькою діаграмою спрямованості.

Всі експерти радять по можливості задіяти більш вільний і ресурсномісткий діапазон 5 ГГц, а запропоновані рішення передбачають примусове підключення клієнтів, що підтримують діапазон 5 ГГц, до відповідних точок доступу.

Для ефективного використання радіоспектру у відкритих просторах з великою щільністю абонентів слід обмежити зони дії точок доступу за рахунок застосування спеціалізованих антен малого радіусу дії. Крім того, потрібно відключити низькі канальні швидкості і обробку пакетів абонентів з низьким рівнем сигналу (RX-SOP), а для безшовного роумінгу – забезпечити 20-відсоткове перекриття зон обслуговування сусідніх точок.

Серед заходів, спрямованих на зниження інтерференції, існує здатність (контролера) автоматично управляти потужністю кожної з точок доступу.

Решітки BeamFlex забезпечують формування точкою доступу до декількох тисяч унікальних діаграм спрямованості для кожного окремого клієнта і навіть для кожного пакету даних у відповідності з особливостями радіосередовища в даний момент часу в даному місці.

4. Перш за все необхідно відзначити, що сучасні підходи проектування мереж з високою щільністю ґрунтуються на розумінні того, що основний користувач в такому сценарії це людина з мобільним пристроєм. Загальна кількість присутніх людей в таких місцях дуже велика, тому кількість потенційних користувачів мережі Wi-Fi також може бути великою.

Безпроводова мережа, побудована за традиційним дизайном, не впорається з поставленими завданнями. В результаті вийшли б великі втрати пакетів, велика кількість ретрансмітерів, і, як наслідок – вкрай низька швидкість передачі даних, нестабільна робота сервісів.

Зменшення зон дії точок доступу досягається за рахунок:

— застосування спеціалізованих вузькоспрямованих антен;

— відключення низьких канальних швидкостей (до 12 Мбіт/с);

— відключення обробки пакетів абонентів з низьким рівнем сигналу (RX-SOP);

— зниження потужності передавача;

Захистити зону HD-покриття від паразитного сигналу Wi-Fi. Негативні явища на покриття глядацької зони чаші стадіону можу надати свої ж точки, розташовані в VIP-зонах, вестибюлях поблизу виходів на поле. Рецепт той же – контроль потужності і радіопокриття.

Скоротити утилізацію радіоканалу: не використовувати більше чотирьох SSID (в ідеалі використовувати один) в зорових зонах, тому що кожен SSID вимагає відправки окремого Beacon пакету і кожен широкомовний SSID відповідає на null probe request.

2 ДОСЛІДЖЕННЯ МЕРЕЖ 3,4,5 ПОКОЛІННЯ, ЯК ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ ДОСТУПУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ

2.1 Принципи функціонування безпроводових мереж 3,4,5 G

3G - це стільникові мережі третього покоління, в яких доступні швидкості передачі даних 384 кбіт/с і вище (в залежності від використовуваної технології). Мережі з технологією 3G використовують UMTS (Universal Moblle Telecommunications Service), FDD (Frequency Division Duplex), TDD (Time Division Duplex), CDMA2000 lx, EV-DO, CDMA2000 3x, TD-CDMA, Arib WCDMA, EDGE (Enhanced Datarate for Global Evolution) і IMT-2000 DECT., Технологія FDD означає, що для вхідного та вихідного зв'язку використовуються різні пари каналів (частот). У технології TDD для вхідного і вихідного зв'язку використовується один канал (частота); 4G, або четверте покоління зв'язку-це нове слово в розвитку технологій. До теперішнього часу основні дослідження в даній області вже закінчено, проте немає вільних частот, на яких могли б працювати дані системи. Основною технологією, що використовується в даних мережах, є мультиплексування з ортогональним частотним розділенням сигналів (OFDM - Orthogonal Frequency Division Multiplexing).

UMTS - одна з технологій 3G, розроблена спільно зі структурою ITU IMT-2000. UMTS - це радіостандарт пакетної передачі даних, що дозволяє передавати текст, оцифрований голос, відеозображення і іншу мультимедійну інформацію зі швидкістю до 2 Мбіт/с. UMTS пропонує користувачам послідовний набір послуг незалежно від того, в якій частині земної кулі вони знаходяться. UMTS заснований на стандарті GSM, що підтверджується стандартами і розробниками. Коли доступ до мережі UMTS буде відкритий в будь-якому географічному місці, абоненти зможуть отримати доступ до мережі Інтернет навіть під час подорожей. Перебуваючи в роумінгу, абоненти матимуть точно такий же набір послуг, як якщо б вони знаходилися у себе вдома. Абоненти будуть отримувати доступ до послуг зв'язку через наземні

з’єднання і супутникові передачі, але тільки тоді, коли система буде повністю введена в дію. Поки систем~ UMTS повністю не добудована, абоненти отримують доступ до послуг зв’язку за допомогою мультирежимних пристроїв, які можуть перемикатися в режим роботи в мережах GSM 900 і 1800 в тих місцях, де UMTS ще не функціонує. Площа покриття UMTS повинна включати в себе всю поверхню земної кулі у вигляді майбутніх наземних телекомунікаційних сервісів, званих IMT2000.

Площа покриття системи UMTS буде забезпечуватися комбінацією стільників з різними зонами покриття, починаючи з пікостільників і закінчуючи великими стільниками, включаючи підтримку з супутника, що забезпечить покриття всієї земної кулі.

UMTS відрізняється від існуючих мереж другого покоління наступними характеристиками:

— більш високу якість мови, ніж в існуючих цифрових мережах. Це мультимедійна мережа, що дозволяє передавати на високій швидкості як голосовий трафік, так і інші види інформації;

— UMTS побудована на базі існуючих мобільних систем 2G, так як вони мають потенціал для передачі даних на швидкості 2 Мбіт/с;

— UMTS є дійсно глобальною системою, що забезпечує зв’язок як наземними засобами, так і супутниковими;

— UMTS пропонує постійне обслуговування, навіть при знаходженні в роумінгу. При знаходженні поза домашньої мережі користувачеві будуть надані всі сервіси. Це відбуватиметься завдяки широкій наземній мережі, а також підтримці з супутників.

Мережі UMTS можуть працювати спільно з мережами GSM/GPRS. Ці дві системи використовують різні частотні діапазони, таким чином, базові станції та мобільні телефони різних мереж не будуть викликати інтерференцію одна з одною. Деякі оператори заявляють, що їх мережі (MSC/HLR/SGSN) і BSC/RNC сумісні з UMTS, але більшість операторів припускають, що мережі повинні бути побудовані окремо від UMTS. Деякі з останніх базових станцій GSM

можуть працювати спільно з UMTS, використовуючи одну вишку. На рис. 2.1 показані етапи переходу системи GSM до UMTS через GPRS і EDGE [8].

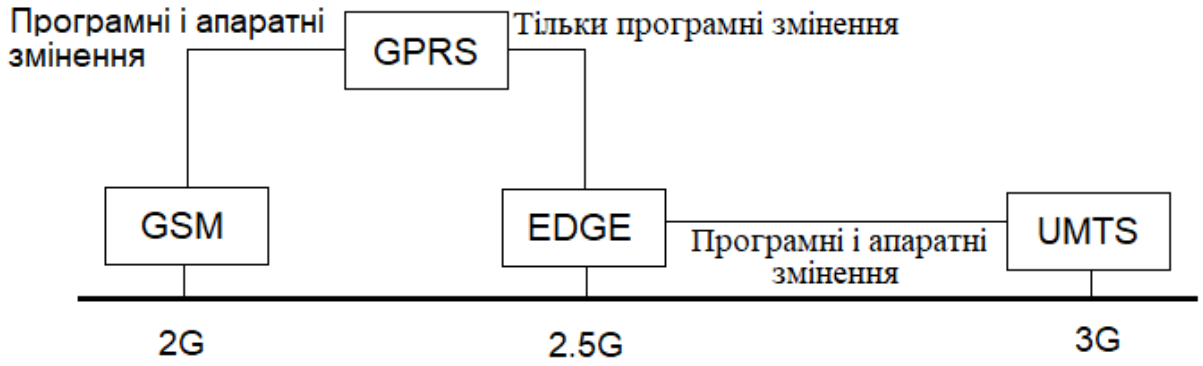

Рисунок 2.1 – Послідовний перехід від GSM до UMTS

Швидкість передачі даних для мереж UMTS може досягати 2 Мбіт/сек. Завдяки технології HSDPA-High Speed Downlink Packet Access (3.5 G), яка була впроваджена в 2006 році максимальна швидкість зросла до 14 Мбіт/с. Ці та інші переваги UMTS дозволяють надавати абонентам широкий перелік послуг: відеодзвінки, відеоконференції, високоякісні голосові дзвінки, завантаження файлів з високою швидкістю, мережеві ігри, мобільну комерцію тощо.

Розглянемо структуру системи UMTS і її основні відмінності від стандарту другого покоління GSM.

Підсистема комутації

У перших релізах стандарту UMTS (R99, R4) підсистема комутації не відрізнялася за своєю структурою від тієї ж підсистеми мереж другого покоління. До неї входили MSC – Mobile Switching Centre, який виконував функції комутації, встановлення з'єднання, тарифікації тощо, а також ряд регістрів HLR, VLR, AUC, які призначені для зберігання абонентських даних. У пізніших релізах (R5, R6, R7,R8) функції MSC були розділені між двома пристроями: MSC-Server і MGW (Media gateway). MSC-Server відповідає за встановлення з'єднань, тарифікацію, виконує деякі функції автентифікації. MGW представляє собою комутаційне поле, підпорядковане MSC-Server.

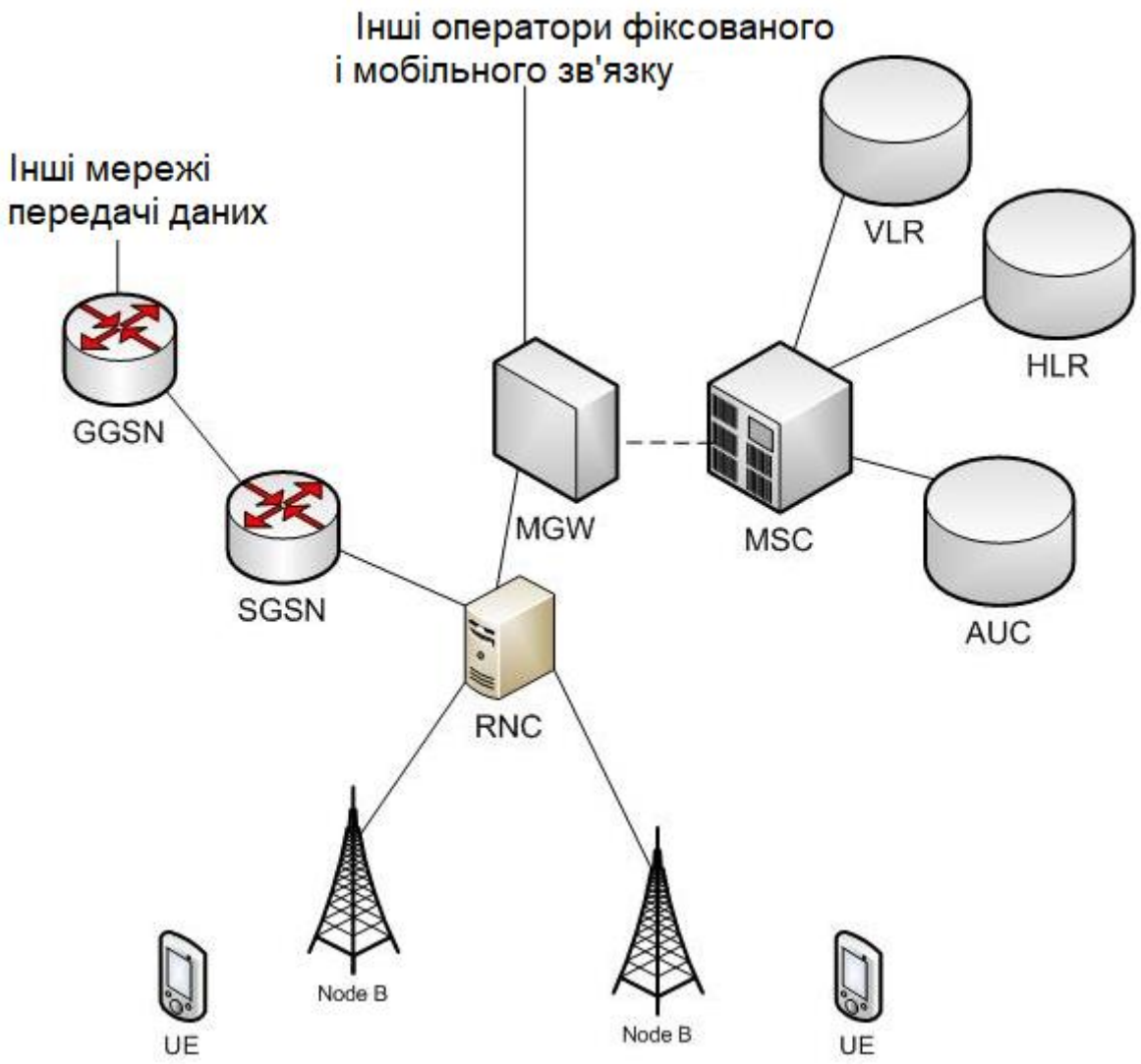

Рисунок 2.2 – Структура мережі стандарту UMTS

Підсистема базових станцій

У мережі UMTS в порівнянні з мережею GSM найбільші зміни зазнала підсистема базових станцій. Зазначені вище переваги досягаються в першу чергу за рахунок нової технології передачі інформації між базовою станцією і телефоном абонента.

Отже, розглянемо основні елементи, що входять в підсистему базових станцій:

RNC (Radio Network Controller) – контролер мережі радіодоступу системи UMTS. Він є центральним елементом підсистеми базових станцій і виконує

більшу частину функцій: контроль радіоресурсу, шифрування, встановлення з'єднань через підсистему базових станцій, розподіл ресурсів між абонентами тощо. В мережі UMTS контролер виконує набагато більше функцій, ніж в системах стільникового зв'язку другого покоління.

NodeB – базова станція системи стільникового зв'язку стандарту UMTS. Основною функцією NodeB є перетворення сигналу, отриманого від RNC в широкосмуговий радіосигнал, що передається до телефону. Базова станція не приймає рішень про виділення ресурсів, про зміну швидкості до абонента, а лише служить мостом між контролером і обладнанням абонента, і вона повністю підпорядкована RNC.

Обладнання абонента отримало назву UE (User Equipment). Тим самим підкреслюється, що на відміну від попередніх стандартів в UMTS може бути не тільки звичайний телефон, але і смартфон, ноутбук, стаціонарний комп'ютер тощо.

Пакетні дані в мережі UMTS передаються від MGW до відомого нам по системі GSM елементу SGSN, після чого через GGSN надходять до інших зовнішніх мереж передачі даних, наприклад Internet. Як правило, SGSN і GGSN мережі GSM застосовуються для тих же цілей і в мережі UMTS. Проводиться тільки корекція програмного забезпечення даних елементів [10].

WiMAX

Стандарт 802.16 - це доповнення стандарту IEEE 802.16, який був виданий у квітні 2002 року і працює на частотах від 10 до 66 ГГц. Ці частотні діапазони полегшують можливість з'єднання з допомогою радіочастот, роблячи технологію WiMAX ідеальним рішенням для використання в якості останньої милі. Зазвичай на шляху радіохвиль присутні перешкоди, такі як дерева або будівлі, а базові станції WiMAX можна розмістити на дахах будівель, а не будувати для цього додаткові вишки.

Більшість конфігурацій WiMAX включають установку базової станції на дах будівлі або вишку, яка буде обслуговувати велику кількість абонентів. Максимальна дальність дії WiMAX становить 50 кілометрів, однак радіус

стільника буде становити від 6 до 10 кілометрів, причому в цьому радіусі не буде обмежень в роботі і пропускної здатності.

В 802.16 також є можливість створення безпроводової технології підключення безпроводових точок доступу 802.11 до мережі Інтернет. Це являє можливість установки хот спотів в тих місцях, де раніше їх було неможливо поставити з-за відсутності провідних ліній зв'язку. Таким чином, оператори зв'язку можуть розширить зону свого впливу, особливо в тих регіонах, де кабельні мережі або DSL просто недоступні.

З роздільною швидкістю передачі даних на кожен сектор базової станції 802.16, де сектор є окремим приймачем-передавачем, забезпечується достатній діапазон для одночасного обслуговування понад 60 виділених ліній зв'язку зі швидкістю, відповідної рівню T1, і сотні домашніх ліній зі швидкістю DSL з'єднання, при використанні каналів шириною 20 МГц. Для підтримки різних моделей оператори зв'язку можуть забезпечувати як високошвидкісні з'єднання ділових абонентів, так і низькошвидкісні підключення відокремлених користувачів. Специфікація 802.16 включає підтримку високої безпеки підключення і якості сервісу (QoS), при цьому забезпечуючи низький час затримки передачі таких даних, як відео або голос. Голосовий сервіс 802.16 може бути здійснений традиційним методом мультиплексування з тимчасовим поділом (TDM) або за допомогою VolP (Voice over IP).

Мережева архітектура WiMAX

Використовуючи стійку схему модуляції, WiMAX забезпечує високу пропускну здатність мережі поряд з високим рівнем ефективності використання спектру, що є допустимим для розгалуженого ослаблення. Динамічна адаптивна модуляція дозволяє базовим станціям WiMAX регулювати швидкість передачі інформації. Наприклад, якщо базова станція не може встановити стійке з'єднання з віддаленим абонентом, використовуючи найвищу схему модуляції, 64 QAM, то модуляція буде знижена до 16 QAM або до чотирифазної ключової модуляції (quadrature phase shift keying : QPSK), яка зменшить пропускну здатність, але збільшить ефективний діапазон дії. Для полегшення планування

розміщення стільників в ліцензованих і неліцензованих діапазонах радіоспектру, WiMAX підтримує гнучкий поділ каналів, що сприяє розширенню мережі. Наприклад, якщо оператор зв'язку використовує 20 МГц спектра, то він може розділити його на два сектори по 10 МГц або на чотири по 5 МГц кожен.

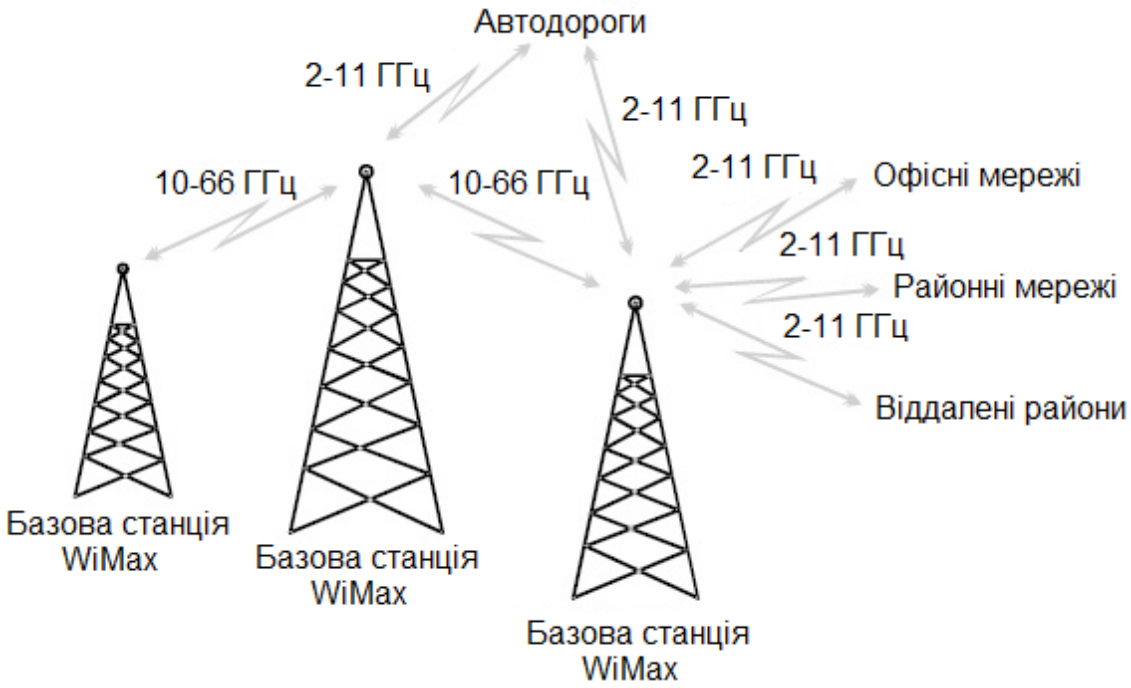

Рисунок 2.3 – Архітектура WiMAX

Сконцентрувавши потужність радіовипромінювання на одному окремому секторі, оператор зв'язку може збільшити в ньому число абонентів при одночасному збільшення дальності дії і пропускної здатності. Для того щоб ще більше збільшити охоплення, оператор може повторно використовувати один і той же спектр в різних секторах, попередньо ізолювавши їх один від одного (шляхом виділення окремих антен для кожного сектора) для того, щоб уникнути інтерференції. Іншими словами, WiMAX дозволяє при певній обережності повторно використовувати частоти. Крім підтримки динамічно змінюваної схеми модуляції стандарт IEEE 802.16 підтримує технології інтелектуальних антен і технології, які збільшують зону покриття, кільцеву топологію. Оскільки відбувається постійне поліпшення радіотехнологій і

падіння вартості, збільшуються можливості для забезпечення високої пропускної спроможності шляхом використання декількох антен для прийому і передачі сигналу, що, в свою чергу, збільшує дальність їх дії. Для захисту переданих даних, автентифікації, стандарт 802.16 забезпечує необхідні рівні захисту і кодування [8].

Загальна структура мережі LTE

Створення конкурентної технології побудови мереж мобільного зв'язку на основі мережі мобільного зв'язку WiMAX (стандарт IEEE 802.16e) активізувало зусилля учасників проекту 3GPP по розробці на основі технології OFDM еволюційного варіанту мережі UMTS, названого LTE.

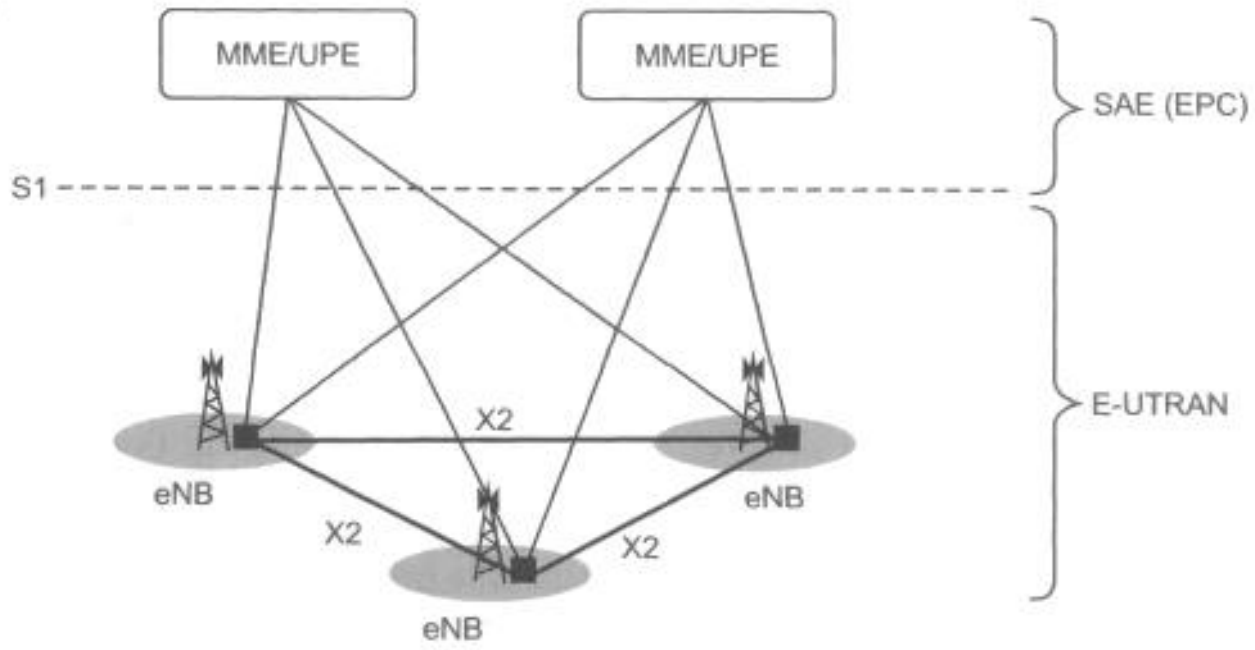

Рисунок 2.4 – Взаємодія мережі радіодоступу E-UTRAN
і базової станції SAE [9]

Мережа LTE складається з двох найважливіших компонентів: мережі радіодоступу E-UTRAN та базової мережі SAE (System Architecture Evolution)

Основними вимогами проекту 3GPP до мережі SAE були: максимально імовірне спрощення структури мережі та виключення дублюючих функцій мережевих протоколів, характерних для системи UMTS.

Мережа радіодоступу E-UTRAN розглянута в ряді технічних специфікацій, згідно з якими вона складається тільки з базових станцій eNB (evolved Node B). Базові станції eNB є елементами мережі E-UTRAN і з'єднані між собою за способом «кожен з кожним» за допомогою інтерфейсу X2. Інтерфейс X2 підтримує хендовер мобільного терміналу в стані LTE_ACTIVE. Кожна базова станція має інтерфейс S1 з базовою мережею SAE, побудованої за способом комутації пакетів.

Базова мережа SAE, іноді звана мережею EPC (Evolved Packet Core), має вузли MME/UPE, що складаються з логічних елементів MMO і UPE. Логічний елемент MMO (Mobility Management Entity) відповідає за вирішення завдань управління мобільністю абонентського терміналу і взаємодіє з базовими станціями eNB мережі E-UTRAN з допомогою протоколів площині управління C-plane (інтерфейс Sl-C). Логічний елемент UPE (User Plane Entity) відповідає за передачу даних користувачів згідно з протоколами площині користувача U-plane і взаємодіє з eNB за допомогою інтерфейсу Sl-U.

Завдяки інтерфейсу SI базові станції з'єднані з декількома вузлами MME/JPE. що дозволяє більш гнучко використовувати мережевий ресурс. Такий інтерфейс називають SI -flex.

Мережа LTE має наступні функціональні відмінності від мережі UMTS.

1. Базові станції eNB виконують функції управління радіоресурсами (Radio Resource Management – RRM): управління радіоканалами (Radio Bearer Control), управління доступом (Radio Admission Control), управління мобільністю (Connection Mobility Control), динамічний розподіл ресурсів (Dynamic Resource Allocation). Таким чином, в мережі радіодоступу E-UTRAN базові станції eNB керують протоколами радіоінтерфейсу, комбінуючи виконання функцій базових станцій Node і більшість функцій контролера RNC мережі UMTS.

2. Мережний елемент керування мобільністю MMO відповідає за розподіл повідомлень виклику (paging) до базових станцій eNB. Крім того, MMO управляє протоколами площини управління: призначення

ідентифікаторів абонентських терміналів, забезпечення безпеки мережі, перевірки автентичності повідомлень абонентів і управління роумінгом.

3. Мережний елемент площині користувача UPE виконує стиснення заголовків IP-протоколів, шифрування потоків даних, комутацію пакетів даних при забезпеченні мобільності користувача. Крім того, UPE управляє протоколами користувацького рівня, наприклад, зберіганням поточного статусу абонентського терміналу (АТ), перериванням на рівні абонентських терміналів.

Одним з найважливіших завдань управління в мережі LTE є максимально ефективне використання радіоресурсів. Дане завдання вирішується за допомогою сукупності функцій управління радіоресурсами RRM (управління радіоресурсами мережі E-UTRAN. управління службою передачі даних в радіоканалі, управління мобільністю, управління доступом, динамічний розподіл ресурсів) і за допомогою протоколу управління радіоресурсами RRC.

Управління радіоресурсами мережі E-UTRAN (Inter Cell RRM) забезпечує управління ресурсами групи стільників з метою підвищення ефективності використання частотного спектра та мінімізації взаємної завади впливу абонентських терміналів та базових станцій, а також підтримку мобільності.

2.2 Рекомендації щодо застосування безпроводових інформаційних технологій в місцях великого скупчення людей

Одне із завдань, пов’язаних з проблемою розширення мережевої інфраструктури, вирішується досить просто. У Європі та Північній Америці збереглися досить багато невикористовуваних оптоволоконних магістралей. З їх допомогою провайдери зможуть тимчасово вирішити проблему надмірного попиту на трафік в проводових мережах.

Однак це не допоможе вирішити проблеми, які виникають через бум безпроводових пристроїв. Мобільний трафік в основному обробляється стільниковими базовими станціями, і його обсяг у середньому зростає на 53%

кожен рік – при тому, що площа покриття станцій не оптимальна, і кожна вежа обслуговує тисячі користувачів.

Мережі стільникового зв'язку першого покоління 1980-х років, які використовували винятково аналоговий сигнал, залишилися в минулому. Мережі другого покоління з'явилися на початку 1990-х років і відрізнялися наявністю цифрових послуг (наприклад, SMS-повідомлень). Лише недавно почалася заміна мереж 2G на більш досконалі технології. Вони все ще складають 75% всіх мереж в Африці і на Близькому Сході. Мережі третього покоління підтримують використання мобільного Інтернету і існують з кінця 1990-х років; зараз їх підтримує більшість мобільних пристроїв Західної Європи.

Таблиця 2.1 – Порівняння швидкостей 3,4,5 покоління

Характеристика	3G	4G	5G
Пікова швидкість(DL)	42 (63) Мбіт	1 Гбіт	>10 Гбіт
Середня швидкість(DL)	3 Мбіт	15 Мбіт	100 Мбіт
Середня затримка	150 мс	50мс	<5 мс
Активних підключень	50/стільник	500/стільник	1 млн/кв.км
Підтримка мобільності	300 км/год	400 км/год	500 км/год

Мережі четвертого покоління поки залишаються найбільш досконалими, вони дозволяють власникам смартфонів користуватися мобільним інтернетом зі швидкістю до 100 Мбіт на секунду. Ця технологія стала доступна в кінці 2000-х років і її популярність швидко зростає. Однак для того, щоб задовольнити рівень попиту на мобільний інтернет, який очікується до 2020-м рокам, знадобиться п'яте покоління безпроводових мереж (5G). І такі мережі повинні

будуть забезпечувати швидкість підключення, що перевершує 4G в сотні разів-десятки Гбіт на секунду.

Сигнал 5G повинен буде поширюватися набагато ширше, ніж це можливо зараз, і охоплювати до мільйона пристроїв на квадратний кілометр. Це буде необхідно для створення «Інтернету речей» – мережі, в яку увійдуть всі види пристроїв, від побутових приладів до систем управління електромережою, медичних пристроїв і автономних автомобілів.

Рисунок 2.5 – Масивна технологія APAA 4G

Об’єднання незалежних телекомунікаційних компаній Third Generation Partnership Project координувало перехід на мережі 3G і 4G, а зараз працює над переходом на 5G. Проводиться випробування технології паралельного вводу-виводу (Multiply Input Multiply Output, MIMO). Вона повинна дозволити одночасну передачу декількох потоків даних на одній радіочастоті. При цьому передавач і приймач обладнуються декількома антенами, і сигнал передається і приймається різними шляхами. Після прийому потоки даних знову поділяються за допомогою складного алгоритму.

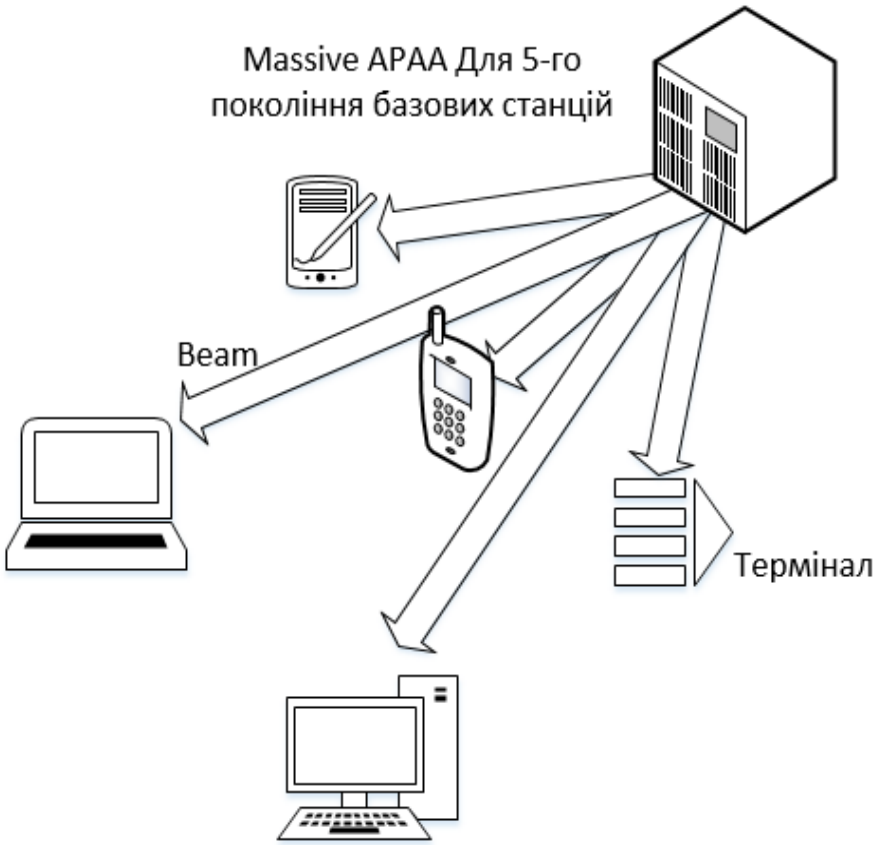

Рисунок 2.6 – Масивна технологія APAA 5G

Технологія MIMO вже застосовується в мережах 4G і Wi-Fi. Проте невеликий розмір смартфона дозволяє встановити лише чотири антени, і стільки ж застосовується на базових станціях. Цю проблему потрібно вирішити в процесі впровадження 5G.

Установки MIMO з великою кількістю антен вже були випробувані. Компанія Ericsson представила багатокористувацьку систему з антеною з 512 елементів на виставці Mobile World Congress. Швидкість передачі даних між стаціонарним і рухомим терміналом досягла 25 Гбіт в секунду. Передача велася на частоті 15 ГГц, яка входить в діапазон високих частот для мереж 5G. Японський стільниковий оператор NTT DoCoMo випробовує систему спільно з Ericsson, а Korea Telecom планує масштабну демонстрацію можливостей 5G під час зимової Олімпіади 2018 року.

Інший підхід передбачає підвищення адаптивності: замість того, щоб використовувати жорстко заданий діапазон частот, мобільний пристрій має

працювати за принципом «когнітивного радіо». При цьому відбувається програмний перехід безпроводового з'єднання на радіоканал, який в даний момент відкрито. Такий метод не тільки дозволить автоматично передавати дані по найшвидшому з можливих маршрутів, але і збільшить стійкість системи. Крім того, він зажадає заміни не апаратного, а програмного забезпечення, що набагато простіше.

Ще одне завдання на шляху до розгортання 5G – резервування діапазону радіочастот для досягнення необхідного покриття і пропускної здатності. Більшість доступних частот вже зарезервовано існуючими міжнародними угодами і застосовується для телемовлення, навігації, у радіотелескопах тощо. Це питання буде розглядатися на Всесвітньої конференції радіозв'язку в 2019 році. Федеральна комісія зі зв'язку США в даний момент розпродає частоти нижче 1 ГГц телекомунікаційним компаніям. Ці частоти раніше були зарезервовані для телемовлення, так як вони краще проникають через перешкоди, чим більш високі, але вони перестали використовуватися після переходу на цифрове ТБ. Використання цих частот оптимально для малонаселеної місцевості та дозволить забезпечити будинки і дороги доступом до 5G за допомогою невеликого числа базових станцій.

Крім того, можливе використання діапазонів з інтервалу 1-6 ГГц у міру заміни мереж 2G і 3G на 5G. Оптимальними ж для густонаселеної міської місцевості вважаються частоти вище 6 ГГц; вони мало використовуються зараз, так як дають невелику дальність проходження сигналу. Планується встановлювати базові станції 5G з інтервалом в 200 метрів. Для порівняння, станції 4G зазвичай встановлюються з інтервалом в 1 км.

Незважаючи на те, що мобільний зв'язок не використовує проводів і її користувачі мобільні, сама по собі мережа мобільного не є. Коли користувач підключається до мережі за допомогою телефону, базова станція перетворює радіосигнал в оптичний сигнал, який потім передається через стаціонарний оптоволоконний кабель.

Вже чверть століття глобальна мережа телекомунікацій будується на каналах з оптоволокна. Його пропускна здатність не порівнянна ні з чим: єдиний кабель товщиною в волосся здатний передавати по 10 Тбіт даних – ємність 25 двошарових Blu-Ray – кожну секунду, і при цьому передавач і приймач можуть стояти на різних берегах Атлантичного океану. Для порівняння-найперший трансатлантичний кабель, проведений в 1988 році, мав пропускну здатність в 30 тис. разів менше. Сучасні технології дозволяють передавати по одному волокну одночасно до 100 окремих сигналів, кожен з яких має власну довжину хвилі. Однак навіть у «оптики» є межі: по мірі того, як сигнал проходить тисячі кілометрів скла, в ньому накопичуються шуми і спотворення. Верхньою межею для одного сигналу вважається швидкість в 100 Гбіт в секунду.

Стандартне оптичне волокно має ядро з надчистого скла товщиною в 9 мікрометрів. Розроблено нове волокно з більш широким ядром, яке менше «забруднює» сигнал шумами, хоча в такому разі воно набагато більш чутливе до розтягування та згинання. Таким чином, «широке» волокно оптимальне для довгих і прямих магістралей – наприклад, підводних кабелів, які знаходяться в стабільному оточенні і не піддаються зовнішнім впливам.

Ширина каналу вкрай важлива, але має значення і швидкодію системи. Людська мова настільки чутлива до переривання, що несподівана пауза в чверть секунди здатна порушити розмову по телефону або відеозв’язку. Для відео також важлива постійна частота кадрів.

Час, який потрібно сигналу для переходу від одного терміналу до іншого, залежить від відстані. Хоча швидкість сигналу в оптичному кабелі становить 200 000 км/с – дві третини швидкості світла в повітрі – затримка між введенням команди, наприклад, в Лондоні, і отриманням відповіді з дата-центру в Сан-Франциско, залишається істотною; в даному випадку вона складе 86 мс. Це обмежує можливості хмарних обчислень. При цьому існує безліч інших нових сервісів – таких як дистанційно керовані роботи і хірургічні операції – які вкрай чутливі до затримок. Не варто забувати і про ігри.

Нові додатки мобільного зв’язку вимагають як швидкого відгуку системи, так і значної ширини каналу. Наприклад, для того, щоб гарантувати безпечну їзду автономного автомобіля, необхідно постійно отримувати дані про місцевість в реальному часі. "Звичайним" автомобілям теж буде потрібно зв’язок з швидким відгуком для систем голосового управління.

Подальший розвиток цієї схеми може відкрити найширші можливості. Наприклад, вона могла б перетворювати сигнал, який отримує вежа 5G від смартфона, в аналоговий оптичний сигнал, який потім можна передати по оптоволокну в центр обробки даних і оцифрувати [11].

Таблиця 2.1 – Сфера застосування 5G технології

Сфера застосування	Ефект
Безпілотні автомобілі	Ліквідація небезпечної затримки сигналу на великій швидкості
Промисловість	Швидкодія промислових роботів і уніфікація інфраструктури
Сільське господарство	Віддалене управління сільгосптехнікою, моніторинг полів тощо
Освіта	Наочне навчання через VR-трансляцію
Телемедецина	Дистанційні операції в реальному часі
Спілкування	Інтерактивна віртуальна реальність
Розваги	Швидка безпроводова передача відео надвисокої чіткості (4К, 8К)
Комп’ютерні ігри	VR - ігри без затримки сигналів

1) Міліметрові хвилі, що дозволяють в десятки разів підвищити швидкість передачі даних, не проникають крізь монолітні перешкоди і швидко затухають в атмосфері. Чим вище частота, тим менше відстань, на якому можлива впевнена передача. Звичайний Wi-Fi роутер на частоті 5 ГГц в

панельному будинку насилу забезпечує зв’язок в одній квартирі. Але менш високі частоти (використовувані в мережах 3G і 4G) вже зайняті.

З одного боку, технологію можна використовувати і в такому вигляді. Наприклад, для забезпечення зв’язку на відкритому стадіоні. Проте в реальних міських умовах прототипи 5G мереж показували незадовільні результати. Вишки, які забезпечували стільниковий зв’язок попередніх поколінь, могли передавати сигнал на велику відстань, а в архітектурі 5G використовують small cells, які раніше застосовувалися у звичайній передавальної техніки для локального посилення сигналу. Максимальна відстань від антени до клієнтського пристрою в цьому випадку навряд чи зможе перевищити сотні метрів.

Зараз "Малі стільники" планується повсюдно встановити в містах: в прив’язці до дахів і стовпів. Поза міст побудова мережі «малих стільників» поки здається недоцільним.

2) Отже, чим вище частота, тим важче сигналу дістатися до клієнтського пристрою без спотворень. Був запропонований підхід, що комбінує можливості сучасних і майбутніх мереж. Йдеться про використання таких технологій передачі даних, як MU-MIMO (Multi-User Multiple Input Multiple Output), SCMA (Sparse Code Multiple Access) і F-OFDM (Filtered OFDM).

Технологія MU-MIMO забезпечує одночасну передачу незалежних потоків даних різним користувачам. Це підвищує ефективність використання частотного спектру, збільшує швидкість передачі даних і кількість одночасних підключень. Раніше MIMO служила для оптимізації LTE і Wi-Fi, але тільки для двох-чотирьох потоків сигналів. У 5G використовують технологію Massive MIMO, що дозволяє розміщувати десятки маленьких антен в мобільних пристроях і сотні – в передавальних станції. Конфігурація станції Massive MIMO включає 128 антен. Для порівняння звичайна станція оснащена 8 антенами – очевидно, що зі збільшенням числа антен технологія дає більш вражаючий результат.

Massive MIMO дозволяє адаптувати передачу сигналу в умовах висотних будівель. Передача даних здійснюється із застосуванням складного алгоритму цифрової обробки сигналів, що направляє окремі потоки даних в області простору.

Крім цього різні компанії використовують власні розробки для 5G. Так фахівці Samsung в мережі 5G при русі на швидкості 110 км/год досягли передачі даних на швидкості 1,2 Гбіт/с. Для цього вони використовували «Гібридну адаптивну технологію масивів» (Hybrid Adaptive Array Technology). Ericsson у своїх випробуваннях використовують десятки і сотні антен для передачі безлічі потоків MIMO.

Huawei робить ставку відразу на кілька технологій: F-OFDM і SCMA.

SCMA – метод кодової модуляції сигналів при забезпеченні багатостанційного доступу, заснований на розріджених кодах. Він дозволяє стільнику обслуговувати в 2,7 рази більше користувачів в порівнянні з 4G і знижує затримку в мережі.

F-OFDM сигнал OFDM з універсальною фільтрацією позасмугових випромінювань. Метод OFDM (англ. Orthogonal frequency-division multiplexing-ортогональний частотний поділ каналів з мультиплексуванням) - був запропонований ще в 1966 році. А ось сучасні версії методу пропонують використання в 5G неортогональних сигналів.

3) Слід враховувати, що 5G – це не технологічна панацея, після впровадження якої 4G - і 3G-мережі будуть ліквідовані. Навпаки, мережі попереднього покоління, особливо Wi-Fi, будуть використовуватися в тандемі з 5G. При цьому буде забезпечено безшовне перемикання між мережами з одним пристроєм, однією сім-картою та на одному тарифному плані. Наприклад, технологія License Assisted Access (LAA) вже зараз дозволяє працювати на частотах Wi-Fi, коли ті не задіяні основними споживачами.

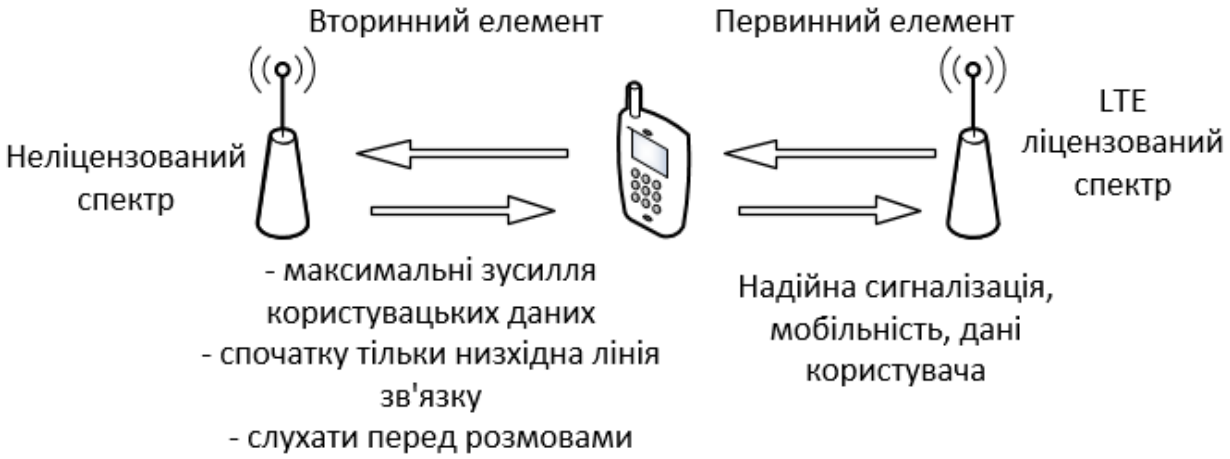

Рисунок 2.7 – Технологія License Assisted Access (LAA)

Більш того, для багатьох завдань цілком достатньо і 4G: наприклад, для класичного взаємодії між користувачами і навіть для роботи IoT-пристроїв, які передають невеликі обсяги інформації і рідко. Вони не вимагають високошвидкісних підключень і можуть працювати з мережами невисокої пропускної здатності.

4) Федеральна комісія зі зв’язку США дозволила установку тестових базових станцій і вишок без спеціального узгодження. Це заощадить розробникам зв’язку п’ятого покоління час на будівництво тестових мереж.

В липні 2016 року комісія відкрила наступні діапазони для використання в мережах 5G: 28 ГГц (27,5-28,35 ГГц), 37 ГГц (37-38,6 ГГц), 39 ГГц (38,6-40 ГГц), 64-71 ГГц (залишивши можливість у майбутньому додати частоти вище 95 ГГц). США стала першою країною, що надала операторам зв’язку таку можливість.

Корпорації також ведуть інтенсивні роботи. Nokia виступила із заявою, що вже підготувала базові станції AirScale Radio Access, які повністю підтримують 5G. Велика частина функціональності цих станцій реалізовано програмно.

У 2016 році в Канаді-Bell спільно з Nokia успішно завершили перші випробування роботи безпроводових мобільних мереж п’ятого покоління. У цьому експерименті використовувався діапазон 73 ГГц.

Також цього року Vodafone і Huawei провели тестування технології 5G, розігнавши мережу до 20 Гбіт/с (для одного пристрою). Тести охоплювали однокористувацьку SU-MIMO (Single User Multiple Input Multiple Output) і багатокористувацьку MU-MIMO (Multi User Multiple Input Multiple Output) передачу даних в діапазоні частоти 71-76 ГГц, 81-86 ГГц і 92-95 ГГц.

Компанія Ericsson на початку року показала перше пристрій, що підтримує 5G. Це 150-кілограмовий телефон, з експериментальними компонентами, який живиться від величезної батареї. Наступний крок – мініатюризації апарату. В Ericsson також заявили, що досягли стійкого прийому сигналу на швидкості 7 Гбіт/с в рухомому автомобілі за допомогою MU-MIMO і Beamforming [11].

Висновки до розділу

1. 3G - це стільникові мережі третього покоління, в яких доступні швидкості передачі даних 384 кбіт/с і вище (в залежності від використовуваної технології). Мережі з технологією 3G використовують UMTS (Universal Moblle Telecommunications Service), FDD (Frequency Division Duplex), TDD (Time Division Duplex), CDMA2000 lx, EV-DO, CDMA2000 3x, TD-CDMA, Arib WCDMA, EDGE (Enhanced Datarate for Global Evolution) і IMT-2000 DECT.,

4G, або четверте покоління зв’язку-це нове слово в розвитку технологій. До теперішнього часу основні дослідження в даній області вже закінчено, проте немає вільних частот, на яких могли б працювати дані системи. Основною технологією, що використовується в даних мережах, є мультиплексування з ортогональним частотним розділенням сигналів (OFDM - Orthogonal Frequency Division Multiplexing).

2. Одне із завдань, пов’язаних з проблемою розширення мережевої інфраструктури, вирішується досить просто. У Європі та Північній Америці збереглися досить багато невикористовуваних оптоволоконних магістралей. З

їх допомогою провайдери зможуть тимчасово вирішити проблему надмірного попиту на трафік в проводових мережах.

Однак це не допоможе вирішити проблеми, які виникають через бум безпроводових пристроїв. Мобільний трафік в основному обробляється стільниковими базовими станціями, і його обсяг у середньому зростає на 53% кожен рік – при тому, що площа покриття станцій не оптимальна, і кожна вежа обслуговує тисячі користувачів.

Мережі четвертого покоління поки залишаються найбільш досконалими, вони дозволяють власникам смартфонів користуватися мобільним інтернетом зі швидкістю до 100 Мбіт на секунду.

Об’єднання незалежних телекомунікаційних компаній Third Generation Partnership Project координувало перехід на мережі 3G і 4G, а зараз працює над переходом на 5G. Проводиться випробування технології паралельного вводу-виводу (Multiply Input Multiply Output, MIMO). Вона повинна дозволити одночасну передачу декількох потоків даних на одній радіочастоті. При цьому передавач і приймач обладнуються декількома антенами, і сигнал передається і приймається різними шляхами. Після прийому потоки даних знову поділяються за допомогою складного алгоритму.

Ще одне завдання на шляху до розгортання 5G – резервування діапазону радіочастот для досягнення необхідного покриття і пропускної здатності. Більшість доступних частот вже зарезервовано існуючими міжнародними угодами і застосовується для телемовлення, навігації, у радіотелескопах тощо.

Massive MIMO дозволяє адаптувати передачу сигналу в умовах висотних будівель. Передача даних здійснюється із застосуванням складного алгоритму цифрової обробки сигналів, що направляє окремі потоки даних в області простору.

3 ЗАХИСТ ІНФОРМАЦІЇ В БЕЗПРОВОДОВИХ МЕРЕЖАХ І ЙОГО ВПЛИВ НА ЯКІСТЬ НАДАННЯ ІНФОРМАЦІЙНИХ ПОСЛУГ

3.1 Системи захисту інформації і їх надійність в мережі Wi-Fi

Нещодавно Wi-Fi Alliance оприлюднив найбільше оновлення безпеки Wi-Fi за останні 14 років. Протокол безпеки Wi-Fi Protected Access 3 (WPA3) вводить дуже потрібні оновлення в протокол WPA2, представлений в 2004 році. Замість того, щоб повністю переробити безпеку Wi - Fi, WPA3 концентрується на нових технологіях, які повинні закрити щілини, що почали з’являтися в WPA2.

Wi-Fi Alliance також оголосив про два додаткових, окремих протоколах сертифікації, що вводяться в дію паралельно WPA3. Протоколи Enhanced Open і Easy Connect не залежать від WPA3, але покращують безпеку для певних типів мереж і ситуацій.

Всі протоколи доступні для впровадження виробниками в їх пристрої. Якщо WPA2 можна вважати показником, то ці протоколи в кінцевому підсумку будуть прийняті повсюдно, але Wi-Fi Alliance не дає ніякого графіка, за яким це повинно відбуватися. Швидше за все, з впровадженням нових пристроїв на ринку ми в результаті досягнемо етапу, після якого WPA3, Enhanced Open і Easy Connect стануть новими опорами безпеки.

Приблизний опис чотирьох основних змін, які вони принесуть із собою в справу безпроводової безпеки.

Одночасна аутентифікація рівних [Simultaneous Authentication of Equals, SAE]

Найбільша зміна, яка принесе WPA3. Найголовніший момент в захисті мережі настає, коли новий пристрій намагається встановити з’єднання. Ворог повинен залишатися за воротами, тому WPA2 і WPA3 приділяють багато уваги автентифікації нових сполук і гарантії того, що вони не будуть спробами хакера отримати доступ.

SAE-новий метод автентифікації пристрою, що намагається підключитися до мережі. SAE – це варіант dragonfly handshake, що використовує криптографію для запобігання вгадування пароля зловмисником. Він говорить про те, як саме новий пристрій, або користувач, має «вітати» мережевий маршрутизатор при обміні криптографічними ключами.

SAE йде на заміну методу Pre-Shared Key (PSK), використовуваного з моменту презентації WPA2 в 2004-м. PSK також відомий, як чотирьох етапне встановлення зв'язку, оскільки саме стільки повідомлень, або двосторонніх актів обміну інформацією, необхідно зробити між маршрутизатором і приєднуваним пристроєм, щоб підтвердити, що вони узгодили процедуру щодо узгодження пароля, при тому, що жодна зі сторін не повідомляє його інший. До 2016 року PSK здавався безпечною, а потім була відкрита атака з перезавантаженням ключа (Key Reinstallation Attacks, KRACK).

Як випливає з назви, SAE працює на підставі припущення про рівноправність пристроїв, замість того, щоб вважати, що один пристрій відправляє запити, а другий – встановлює право на підключення (традиційно це були пристрої, які намагалися з'єднати, і маршрутизатор, відповідно). Будь-яка із сторін може відправити запит на з'єднання, і потім вони починають незалежно відправляти інформацію, замість того, щоб обмінюватися повідомленнями по черзі, туди-сюди. А без такого обміну у атаки KRACK не буде можливості перешкодити, і атаки за словником стануть марними.

SAE пропонує додаткове посилення безпеки, якого не було в PSK: пряму секретність(forward secrecy). Припустимо, атакуючий отримує доступ до зашифрованих даних, які маршрутизатор відправляє і отримує з інтернету. Раніше атакуючий міг зберегти ці дані, а потім, в разі успішного підбору пароля, розшифрувати їх. З використанням SAE при кожному новому з'єднанні встановлюється новий шифрувальний пароль, тому навіть якщо атакуючий в якийсь момент і потрапить в мережу, він зможе вкрасти пароль від даних, переданих після цього моменту.

KRACK перериває серію двосторонніх актів обміну інформацією, прикидаючись, що з’єднання з маршрутизатором тимчасово перервалося. Насправді він використовує повторювані можливості з’єднання для аналізу двосторонніх актів обміну інформацією, поки не зможе здогадатися про те, який був пароль. SAE блокує можливість такої атаки, а також найбільш поширені офлайнові атаки по словнику, коли комп’ютер перебирає мільйони паролів, щоб визначити, який з них підходить до інформації, отриманої під час PSK-з’єднань.

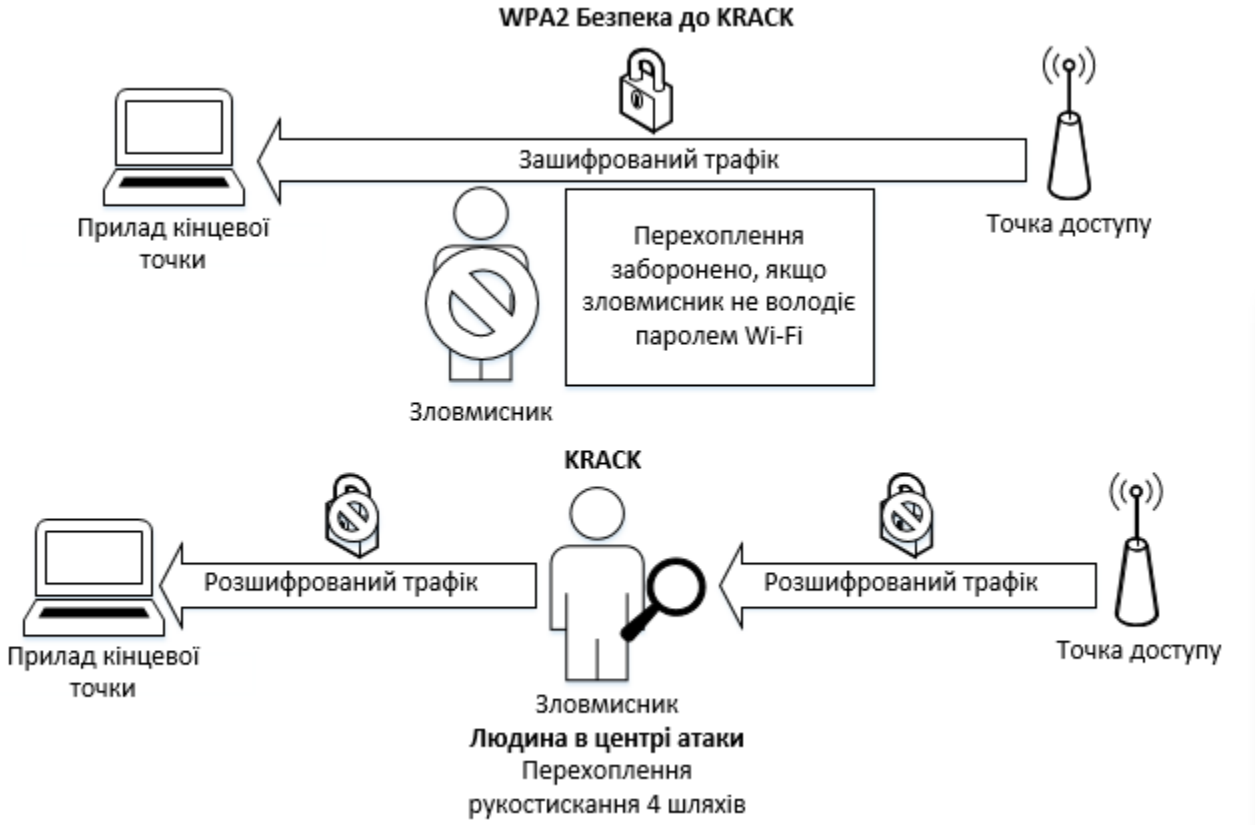

Рисунок 3.1 – Принцип роботи з KRACK і без нього

192-бітові протоколи безпеки

WPA3-Enterprise, версія WPA3, призначена для роботи в урядових і фінансових установах, а також в корпоративному середовищі, володіє шифруванням в 192 біта. Такий рівень шифрування для домашнього

маршрутизатора буде надмірним, але сенс використовувати його в мережах, що працюють з особливо чутливою інформацією.

Зараз Wi-Fi працює з безпекою в 128 біт. Безпека в 192 біта не буде обов'язковою для використання – це буде варіант налаштувань для тих організацій, мереж яких вона буде потрібна. Wi-Fi Alliance також підкреслює, що в промислових мережах необхідно посилювати безпеку на всіх фронтах: стійкість системи визначається стійкістю найслабшої ланки.

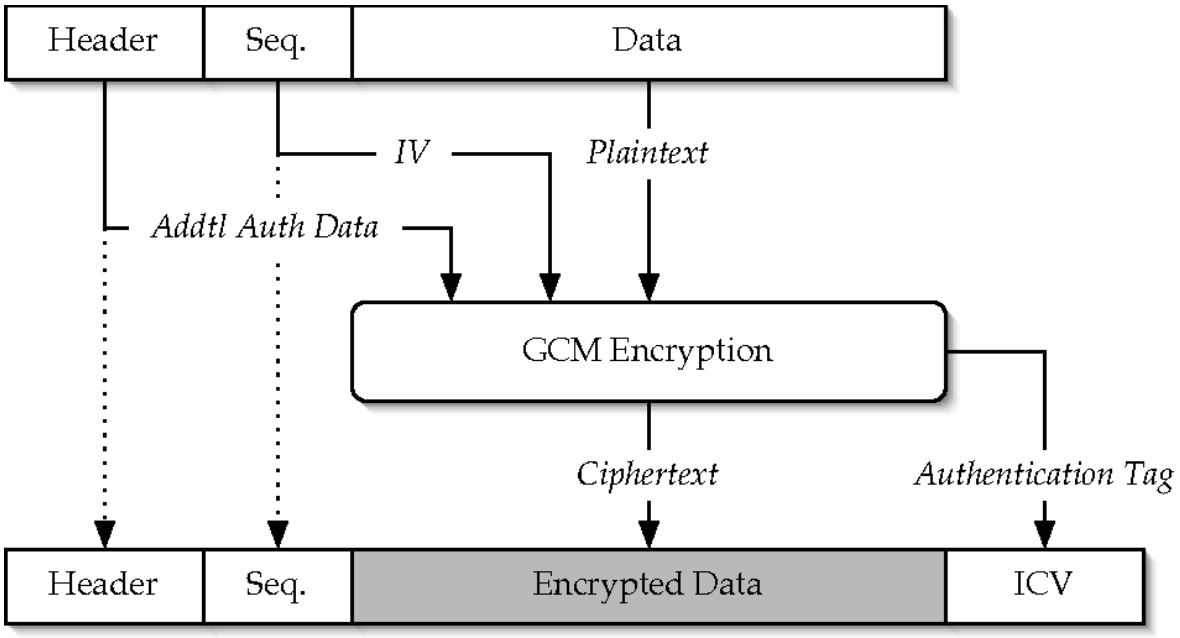

Рисунок 3.2 – 256-бітний протокол Galois/Counter Mode

Щоб гарантувати належний рівень безпеки всієї мережі, від початку до кінця, WPA3-Enterprise буде використовувати 256-бітний протокол Galois/Counter Mode для шифрування, 384-бітний Hashed Message Authentication Mode режим для створення і підтвердження ключів, і алгоритми Elliptic Curve Diffie-Hellman exchange, Elliptic Curve Digital Signature Algorithm для аутентифікації ключів. У них багато складної математики, але плюс в тому, що на кожному кроці буде підтримуватися шифрування в 192 біта.

Easy Connect

Easy Connect – це визнання наявності в світі величезної кількості пристроїв, приєднаних до мережі. І хоча, можливо, не всі люди захочуть

обзавестися розумними будинками, у середньої людини до домашнього маршрутизатора сьогодні, швидше за все, підключено більше пристроїв, ніж у 2004 році. Easy Connect – спроба Wi-Fi альянсу зробити приєднання всіх цих пристроїв більш інтуїтивним.

Замість того, щоб кожен раз при додаванні пристрою вводити пароль, у пристроїв будуть унікальні QR-коди – і кожен код пристрою буде працювати як публічний ключ. Для додавання пристрою можна буде просканувати код за допомогою смартфона, вже з'єднаного з мережею.

Після сканування пристрій обмінюється з мережею ключами автентифікації для встановлення подальшого зв'язку. Протокол Easy Connect не пов'язаний з WPA3 – пристрої, сертифіковані для нього, повинні мати сертифікат для WPA2, але не обов'язково сертифікат для WPA3.

Рисунок 3.3 – Протокол Easy Connect

Enhanced Open

Enhanced Open – ще один окремий протокол, розроблений для захисту користувача у відкритій мережі. Відкриті мережі – такі, якими ви користуєтеся в кафе або аеропорту – несуть у собі цілий комплекс проблем, які зазвичай не стосуються вас, коли ви встановлюєте з'єднання вдома або на роботі.

Багато атак, що відбуваються у відкритій мережі, відносяться до пасивних. Коли до мережі підключається купа людей, атакуючий може зібрати дуже багато даних, просто фільтруючи інформацію.

Enhanced Open використовує опортуністичне безпроводове шифрування (Opportunistic Wireless Encryption, OWE), визначена в стандарті Internet

Engineering Task Force RFC 8110, щоб захищатися від пасивного підслуховування. Для OWE не потрібен додатковий захист з автентифікацією- воно концентрується на поліпшенні шифрування даних, що передаються по публічних мережах, з метою запобігти їх крадіжці. Воно також запобігає простій ін'єкції пакетів (unsophisticated packet injection), в якій атакуючий намагається порушити роботу мережі, створюючи і передаючи особливі пакети даних, що виглядають, як частина нормальної роботи мережі.

Enhanced Open не дає захисту з автентифікацією через особливості організації відкритих мереж - вони за визначенням призначені для загального використання. Enhanced Open був розроблений для поліпшення захисту відкритих мереж проти пасивних атак, так, щоб не вимагати від користувачів введення додаткових паролів або проходження додаткових кроків.

Пройде, щонайменше, кілька років, до того, як WPA3, Easy Connect і Enhanced Open стануть нормою. Широке поширення WPA3 відбудеться тільки після заміни або оновлення маршрутизаторів. Однак якщо вас турбує безпека вашої особистої мережі, ви зможете замінити свій поточний маршрутизатор на інший, який підтримує WPA3, як тільки виробники почнуть продавати їх, що може статися вже через кілька місяців [12].

3.2 Системи захисту інформації і їх надійність в мережі 5G

Мережі п'ятого покоління будуть одночасно і схожі на будь-яке попереднє покоління мобільних мереж, і при цьому помітно відрізнятися від них, і цьому є цілий ряд пояснень, які стають очевиднішими, якщо задуматися про те, яким чином ці зміни впливають на принципи забезпечення безпеки користувачів та обладнання в екосистемі мереж п'ятого покоління.

На відміну від існуючих рішень, які змушені жертвувати продуктивністю при використанні поточних безпроводових технологій (3G, 4G, Wi-fi, Bluetooth, Zigbee і тощо), мережі 5G створюються для реального масового впровадження

«інтернету речей» та інших вимогливих до швидкості мережі і доступності сервісів.

Рисунок 3.5 – 5G безпека

1. Мережі 5G мають більше вразливих місць в порівнянні з нинішніми мережами стільникового зв’язку.

Ми поступово йдемо від тієї моделі, коли оператори мобільних мереж отримували від перевірених постачальників відразу комплекс апаратного і програмного забезпечення, і потрапляємо в новий світ віртуалізованої інфраструктури, де використовується цілий «зоопарк» програмного забезпечення, побудованого на базі відкритих вихідних кодів, так і на базі закритих технологій. А це означає, що потенційні вразливі місця в мобільних мережах нового покоління буде мати набагато більше схожості з такою в класичному підприємстві, оскільки стандартні віртуалізовані технології більш доступні і краще відомі зловмисникам, ніж власні мережні технології, які характерні для нинішніх мереж стільникового зв’язку.

2. Розвиток мобільної периферії призводить до змін в периметрі безпеки.

Мережі п’ятого покоління забезпечують набагато більшу ступінь свободи у використанні периферійних ресурсів, які дозволяють зняти частину навантаження з «ядра» мережі – і це дійсно важливо з урахуванням того, що в

мережі з’являється все більше програм, які передбачають мінімальну мережеву затримку, починаючи з ігор з високим дозволом і закінчуючи такими критично важливими додатками як безпілотні автомобілі. Так, мережі 5G дозволяють кешувати контент локально – і якщо вам захочеться подивитися фільм за запитом, додаток може забирати потік з локального кеша, а не передавати його по ядру мережі безпосередньо с серверів контент-провайдера, що в свою чергу вимагає зміни підходів до забезпечення безпеки даних і мережевих комунікацій.

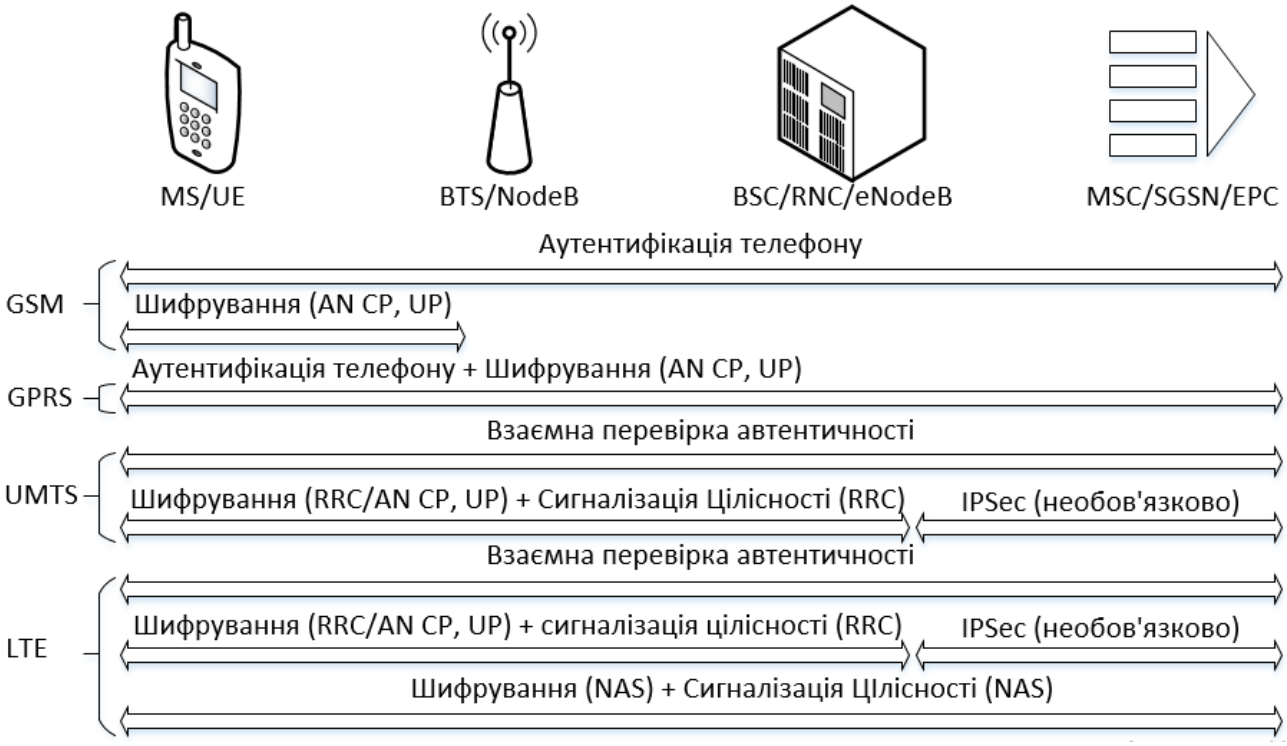

Рисунок 3.5 – Принципи безпеки мереж GSM, GPRS, UMTS, LTE

(AN – Access Network (доступ до мереж); AS – Access Stratum (шар доступу); RRC – Radio Resource Control (управління радіоресурсами); NAS – Non-Access Stratum (шар без доступу); CP – Control Plane (площина управління); UP – User Plane (площа користувача))

3. Поява нових можливостей для створення додаткових рівнів безпеки в каналах стільникового зв’язку.

В даний час основним завданням при забезпеченні безпеки в стільникового зв’язку є захист від прослуховування. Однак в майбутньому світі смартфонів і Інтернету речей, в оточеннях з великою кількістю механізмів, ймовірність прослуховування, по всій видимості, відійде на другий план.

Замість цього нам доведеться задуматися про такі речі як атаки з маніпуляцією даними, які, наприклад, можуть використовуватися для того, щоб віддавати механізмам команди на виконання певних дій (наприклад, відчинити двері або перехопити керування безпілотним автомобілем). У операторів мобільних мереж, як і у виробників побутової електроніки, з'явиться можливість пропонувати «безпеку у вигляді сервісу», у результаті чого постачальники додатків зможуть при передачі окремих видів даних застосовувати додаткові рівні безпеки поверх вже існуючих захищених каналів мережі стільникового зв'язку.

4. Застосування різних механізмів безпеки в залежності від типу даних.

Сьогодні відповідальність за шифрування і захист даних лежить на постачальнику додатків. У мережах 5G певна роль в цьому процесі буде відводитися і операторам мереж-особливо з появою IoT пристроїв, що не володіють достатньою обчислювальною потужністю для достатнього шифрування комунікацій. Постачальники безпеки у вигляді сервісу можуть запропонувати три різних опції захисту в додаток до того, що мережа забезпечує за замовчуванням:

— передачу трафіку без шифрування (для даних, які не мають великої цінності, які, в разі їх перехоплення, будуть фактично марні для зловмисників, наприклад, дані ping-запитів)

— середній рівень захисту (як варіант – для датчиків IoT, дані з яких можна використовувати для атак з підтасовуванням цих даних, наприклад, коли зловмисник може спотворити такі дані, показуючи рівень води в заплаві нижче реального значення і таким чином відключити спрацьовування захисту)

— високий рівень безпеки (де потрібна вища конфіденційність і захист персональної інформації, які актуальні для високо цінних даних, наприклад, при передачі даних кредитних карт в торгових транзакціях).

Все це дозволить розробникам додатків не обмежуватися одними лише платформами смартфонів, і при необхідності вони зможуть реалізувати додатковий рівень безпеки.

5. Забезпечення безпеки в умовах зростання M2M комунікацій.

В цих умовах велике значення має забезпечення конфіденційності і цілісності даних, що передаються між пристроями, оскільки подібні оточення допускають нові види уразливості. Нещодавно ми вже бачили успішні атаки з маніпуляцією даними, в результаті яких дослідникам Keen Security Lab в лабораторних умовах вдалося перехопити керування безпілотним автомобілем Tesla. Слід задуматися про те, як захищати такі дані від подібних атак у всіх фрагментах ланцюга, як в мережі стільникового зв'язку, так і за її межами. Навіть при наявності захищених каналів зв'язку вам може знадобитися забезпечити шифрування переданих через публічну IP мережу даних, коли ці дані залишають мобільну мережу і йдуть за межі операторського шлюзу.

Перш ніж ми побачимо комерційний запуск перших мереж п'ятого покоління, нам ще належить багато чого визначити в області технологій 5G, і треба чимало обговорень проблем безпеки. Починаючи з цього моменту, замість масштабних і дорогих модернізацій на рівні ядра мережі для отримання мереж 6G і новіших технологій, ймовірно, ми будемо мати справу з програмно-визначеним оточенням, в якому застосовні дуже різні правила [13].

Висновки до розділу

1. Найголовніший момент в захисті мережі настає, коли новий пристрій намагається встановити з'єднання. Ворог повинен залишатися за воротами, тому WPA2 і WPA3 приділяють багато уваги автентифікації нових сполук і гарантії того, що вони не будуть спробами хакера отримати доступ.

SAE-новий метод автентифікації пристрою, що намагається підключитися до мережі. SAE – це варіант dragonfly handshake, що використовує криптографію для запобігання вгадування пароля зловмисником.

WPA3-Enterprise, версія WPA3, призначена для роботи в урядових і фінансових установах, а також в корпоративному середовищі, володіє шифруванням в 192 біта.

Щоб гарантувати належний рівень безпеки всієї мережі, від початку до кінця, WPA3-Enterprise буде використовувати 256-бітний протокол Galois/Counter Mode для шифрування, 384-бітний Hashed Message Authentication Mode режим для створення і підтвердження ключів.

Пройде, щонайменше, кілька років, до того, як WPA3, Easy Connect і Enhanced Open стануть нормою. Широке поширення WPA3 відбудеться тільки після заміни або оновлення маршрутизаторів.

2. В даний час основним завданням при забезпеченні безпеки в стільникового зв'язку є захист від прослуховування. Однак в майбутньому світі смартфонів і Інтернету речей, в оточеннях з великою кількістю механізмів, ймовірність прослуховування, по всій видимості, відійде на другий план.

Сьогодні відповідальність за шифрування і захист даних лежить на постачальнику додатків. У мережах 5G певна роль в цьому процесі буде відводитися і операторам мереж-особливо з появою IoT пристроїв, що не володіють достатньою обчислювальною потужністю для достатнього шифрування комунікацій.

4 РОЗРОБЛЕННЯ СТАРТАП-ПРОЕКТУ

4.1 Опис ідеї проекту

Суттю стартапу є: монтаж Wi-Fi мережі в місцях великого скупчення людей. Зміст ідеї та визначення характеристик ідеї стартапу наведедо в табл. 4.1 та табл. 4.2.

Таблиця 4.1 – Зміст ідеї стартап-проекту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Планування та монтаж мережі Wi-Fi у місцях великого скупчення людей	1. Підприємства, компанії, офіси тощо	Швидке планування та монтаж для необхідної роботи на підприємствах тощо
	2. Концерти, стадіони, розваги тощо	Надійна мережа для проведення різних заходів
	3. Міста, райони, Парки тощо	Поширення постійного високоякісного зв’язку у місцях великого скупчення людей

Таблиця 4.2 – Визначення характеристик ідеї проекту

№ п/п	Техніко-економічні характеристики ідеї	Потенційні товари/концепції конкурентів		W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
		Запропо-нований метод	Загально-вживаний метод			
1.	Пропозиція продажу або оренди професійного обладнання для прямих трансяцій	Дає змогу	Дає змогу	Комплект обладнання є габаритним	Рівень цін продажу та оренди не задовольняє звичайного споживача	Рішення є дешевшим ніж аналоги конкурентів
2.	Підвищення якості зв’язку в умовах низького рівня радіопокриття	Дає змогу	Не дає змогу	Не гарантується 100% гарантія успіху проведення мережі	Потребує Додаткових затрат на периферію	Забезпечуєтьс я Високоякісне передавання сигналу

4.2 Технологічний аудит ідеї проекту

У таблиці 4.3 наведено оцінку технологічної здійсненності ідеї проекту та наведено технології, що можуть бути використані для реалізації проекту.

Таблиця 4.3 – Технологічна здійсненність ідеї проекту

№ п/п	Ідея проекту	Технології її реалізації	Наявність технологій	Доступність технологій
1	Організація планування та монтажу Wi-Fi мережі	Спеціалізоване обладнання для монтажу Wi-Fi мережі	Наявна	Доступна
2		Застосування апаратних систем загального призначення	Необхідно розробити	При обмеженому бюджеті недоступна
3		Розробка власних апаратно-програмних рішень	Наявна	При обмеженому бюджеті недоступна

Обрана технологія реалізації ідеї проекту: застосування спеціалізованого обладнання для планування та монтажу Wi-Fi мережі.

4.3 Аналіз ринкових можливостей запуску стартап-проекту

У таблиці 4.4 наведено попередню характеристику потенційного ринку стартап-проекту.

Таблиця 4.4 – Попередня характеристика потенційного ринку стартап-проекту

№ п/п	Показники стану ринку (найменування)	Характеристика
1	Кількість головних гравців, од	10
2	Загальний обсяг продаж, грн/ум.од	350000
3	Динаміка ринку (якісна оцінка)	Зростає
4	Наявність обмежень для входу (вказати характер обмежень)	Зацікавлення потенційних клієнтів

Продовження таблиці 4.4

5	Специфічні вимоги до стандартизації та сертифікації	Ліцензування на монтаж
6	Середня норма рентабельності в галузі (або по ринку), %	350000/280000 = 125%

У таблиці 4.5 наведено характеристику потенційних клієнтів стартап-проекту.

Таблиця 4.5 – Характеристика потенційних клієнтів стартап-проекту

№ п/п	Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
1	Забезпечення стабільності мережного зв’язку	Приватні та державні підриємства, офіси, різні заходи з високою щільністю людей	Рівень очікування якості передавання сигналу	Відповідність результату найвищим стандартам якості
2	Забезпечення передавання сигналу високої чіткості	Приватні та державні підриємства, офіси, різні заходи з високою щільністю людей	Кожна з потенційних цільових груп має свої вимоги до стандартів сигналу	Забезпечення передавання сигналу від рівня потреб споживача

У табл. 4.6 показані фактори загроз реалізації стартап-проекту.

Таблиця 4.6 – Фактори загроз

№ п/п	Фактор	Зміст загрози	Можлива реакція компанії
1	Незацікавленість клієнтів	Внаслідок невдалого маркетингу клієнт може не зацікавитись послугами	Внесення додаткових сервісних послуг
2	Втрата конкуренції	Втрата рангу надійного поставника	Якісне та кількісне нарощування інтенсивності та грамотна цінова політика

У табл. 4.7 наведено фактори можливостей при реалізації стартап-проекту.

Таблиця 4.7 – Фактори можливостей

№ п/п	Фактор	Зміст можливості	Можлива реакція компанії
1	Перехід до домінування на ринку послуг	Зростання попиту	Якісне та кількісне нарощування потужностей
2	Імплементація технологій в існуючій системі	Зростання попиту внаслідок зростання об’ємів закупівель	Якісне та кількісне нарощування потужностей

У таблиці 4.8 визначено особливості конкурентного середовища та його вплив на впровадження проекту [14].

Таблиця 4.8 – Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)
1.Конкуренція	Використання вже існуючих технологій	Стандартизація на високому рівні
2.Локальний	Відсутність єдиного національного постачальника послуг	Окремий підхід до кожної локальної ділянки
3.Міжгалузева	Відсутня	Відсутня
4.Товарно-видова	Застосування стандартизованих технологій	За необхідності, використання загальновживаних апаратних та програмних засобів
5.Цінова	Застосування спеціалізованих комплексів, які мають значну ціну	Можливість заощадити за допомогою застосування загальновживаних апаратних засобів
6.Марочна	Кожна діагностика має бути стандартизованою	Отримання переваги на ринку медійних послуг

У таблиці 4.9 наведено аналіз конкуренції проекта в галузі за М.Портером

Таблиця 4.9 – Аналіз конкуренції в галузі за М. Портером

Складові аналізу	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари- замінники
	Апаратні постачальники	Необхідність пошуку поста-чальників	Залучення малопопулярних постачальників	Неза-лежність у прийнятті клієнтських рішень	Надання переваги більш авторитетним апаратним рішенням
Висновки:	Середня	Можливість виходу на ринок є	Постачальники диктують цінову політику на обладнання	Клієнти диктують вимоги до якості	Обмеження існують лише у разі відмови від діагностики

У табл. 4.10 наведено фактори конкурентоспроможності та їх обґрунтування.

Таблиця 4.10 – Обґрунтування факторів конкурентоспроможності

№ п/п	Фактор конкурентоспроможності	Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проектів значущим)
1	Раціональніший ціновий показник	Можливість більш раціонально використати ресурси на покращення якості сигналу
2	Надання сервісних послуг	Сервісна підтримка апаратної та програмної частини

У табл. 4.11 наведено сильні та слабкі сторони проекту.

Таблиця 4.11 – Порівняльний аналіз сильних та слабких сторін проекту

№ п/п	Фактор конкурентоспроможності	Бали 1-20	Рейтинг товарів-конкурентів у порівнянні						
			–3	–2	–1	0	+1	+2	+3
1	Раціональніший ціновий показник	16		+					
2	Надання сервісних послуг	13			+				
3	Періодична діагностика	8						+	
4	Необхідність залучення висококваліфікованих кадрів	8					+		

Таблиця 4.12 – SWOT- аналіз стартап-проекту

Сильні сторони: раціональний ціновий показник, надання сервісних послуг	Слабкі сторони: періодична діагностика, необхідність залучення висококваліфікованих кадрів
Можливості: Перехід до ексклюзивного застосування нового методу, Імплементація методу в існуючі апаратні комплекси	Загрози: Незацікавленість клієнтів, Втрата монополії

Альтернативи ринкового впровадження стартап-проекту наведені у табл. 4.13.

Таблиця 4.13 – Альтернативи ринкового впровадження стартап-проекту

№ п/п	Альтернатива (орієнтовний комплекс заходів) ринкової поведінки	ність отримання ресурсів	Строки реалізації
1	Укладення договорів з мережними компаніями та швидке захоплення ринку при використанні нового рішення	висока	незначні
2	Використання приладів загального вжитку для підвищення конкурентоспроможності	середня	незначні

4.4 Розроблення ринкової стратегії проекту

Обгрунтування вибору цільових груп потенціійних споживачів наведено у табл. 4.14 [15].

Таблиця 4.14 – Вибір цільових груп потенційних споживачів

№ п/п	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1	Приватні організації і компанії Надання якісних послуг	Середня	Високий	Середня	Середня
2	Офіси та невеликі кафе, ресторани тощо	Низька	Середній	Середня	Висока

Визначення базової стратегії розвитку наведено у табл. 4.15.

Таблиця 4.15 – Визначення базової стратегії розвитку

№ п/п	Обрана альтернатива розвитку проекту	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку*
1	Використання альтернативних технологій та пристроїв	Встановлення нового стандарту якості	Зацікавлення та залучення гігантів у галузі обслуговування мереж віддаленого доступу	Стратегія диференціації
2	Дешевизна проекту	Раціональніші витрати на обладнання, та послуги	Застосування загальновживаних апаратних рішень замість спеціалізованих комплексів	Стратегія лідерства по витратах

Визначення базової стратегії конкурентної поведінки наведено у табл. 4.16.

Таблиця 4.16 – Визначення базової стратегії конкурентної поведінки

№ п/п	Чи є проект «першопрохідцем» на ринку?	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурента, і які?	Стратегія конкурентної поведінки*
1	Ні	Забирати існуючих та шукати нових	Не буде	Стратегія виклику лідера

Визначення стратегії позиціонування наведено у табл. 4.17.

Таблиця 4.17 – Визначення стратегії позиціонування

№ п/п	Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкурентоспроможні позиції власного стартап-проекту	Вибір асоціацій, які мають сформувати комплексну позицію власного проекту (три ключових)
1	Висока якість послуг	Стратегія диференціації	Новизна, гарант якості, точність дослідження	Якість, надійність, точність
2	Мінімальні витрати	Стратегія лідерства по витратах	Універсальність запропонованого рішення	Дешевизна, універсальність

4.5 Розроблення маркетингової програми стартап-проекту

Ключові переваги концепції потенційного товару наведено у табл. 4.18.

Таблиця 4.18 – Визначення ключових переваг концепції потенційного товару

№ п/п	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити
1	Якість	Висока якість, надійність	Надійність
2	Дешевизна	Раціональне використання коштів, дешевше обладнання	Дешевизна

Визначено три рівні моделі товару. Сутність та складові рівнів товару наведено у табл. 4.19.

Таблиця 4.19 – Опис трьох рівнів моделі товару

<table>
<tr><td>Рівні товару</td><td colspan="3">Сутність та складові</td></tr>
<tr><td>І. Товар за задумом</td><td colspan="3">Якісний товар та послуги, стандартизована якість послуг та обладнання</td></tr>
<tr><td rowspan="5">ІІ. Товар у реальному виконанні</td><td>Властивості/характеристики</td><td>М/Нм</td><td>Вр/Тх /Тл/Е/Ор</td></tr>
<tr><td>1)Вартість обслуговування,
2)Кількість комплектів обладнання
3)Строк безвідмовної праці
4)Технологічна собівартість товару</td><td>1) М
2) М
3) М
4) М</td><td>1)Е
2) Пр 3)Нд 4)Тх</td></tr>
<tr><td colspan="3">Якість: міжнародні стандарти якості, постійна підтримка обладнання</td></tr>
<tr><td colspan="3">Доставка, встановлення та налаштування</td></tr>
<tr><td colspan="3">Марка: Інформаційні технології</td></tr>
<tr><td rowspan="2">ІІІ. Товар із підкріпленням</td><td colspan="3">До продажу – обладнання, встановлення</td></tr>
<tr><td colspan="3">Після продажу – сервісна підтримка</td></tr>
</table>

За рахунок чого потенційний товар буде захищено від копіювання: специфічна методика обробки даних.

Визначення меж встановлення ціни на послугу наведено у табл. 5.20.

Таблиця 4.20 – Визначення меж встановлення ціни

№ п/п	Рівень цін на товари-замінники	Рівень цін на товари-аналоги	Рівень доходів цільової групи споживачів	Верхня та нижня межі встановлення ціни на товар/послугу
1	12000 у.о./од. (стандартна методика)	-	Високий	Н.6000 у.о. – В.13000 у.о. (Товар) Н.400 у.о. – В.1500 у.о. (Послуга)

Формування системи збуту послуги наведено у табл. 4.21.

Таблиця 4.21 – Формування системи збуту

№ п/п	Специфіка закупівельної поведінки цільових клієнтів	Функції збуту, які має виконувати постачальник товару	Глибина каналу збуту	Оптимальна система збуту
1	Орієнтована на отримання максимальної якості сигналу	Поставки якісного, точного та надійного товару	Значна	Договірна система збуту

Концепції маркетингових комунікацій наведено у табл. 4.22.

Таблиця 4.22 – Концепція маркетингових комунікацій

№ п/п	Специфіка поведінки цільових клієнтів	Канали комунікацій, якими користуються цільові клієнти	Ключові позиції, обрані для позиціонування	Завдання рекламного повідомлення	Концепція рекламного звернення
1	Зацікавленість в якісному та точному продукті з раціональним використанням ресурсів	Мережні ресурси	Гарантованість якості та стандартизація, політика сервісності	Зацікавити у покращеннях пов’язаних із зростаючою популярністю послуг	Представлення центру синхронізації відправною точкою на шляху до над якісного контенту
2	Зацікавленість у великій кількості продукту із дотриманням умов якісності	Мережні ресурси	Глибина каналу постачальників, гарант якості	Зацікавити у позитивних сторонах первісності та в глибині каналу постачання	Представлення послуг центру синхронізації єдиним раціональним шляхом у забезпеченні стабільного трафіку

Висновки до розділу

1. Комерціалізацію стартап-проекту на рахунок розвитку та впровадження висунутого апаратно-програмного рішення для планування та монтажу Wi-Fi мережі детального аналізу, можна вважати доцільною. На даному ринку інформаційних технологій присутній попит, водночас він задовольняється товарами замінниками та більш коштовними рішеннями, саме тому фундаментально зайняти нішу конкурента, як поставник вигідного продукту, порівнюючи з конкурентами. Рентабельність на ринку послуг передусім обумовлена заміною цілої апаратної залежності на універсальність, що визначена використанням не спеціалізованих комплексів, а загальновживаного апаратного і програмного забезпечення.

2. Впровадження є очікуваним, оскільки основними групами клієнтів є масштабні приватні і державні підприємства, також різні організації заходів з великої щільністю і після набуття достатньої авторитетності можливе охоплення у розмірах міжнаціональних ринків. Конкурентоспроможність проекту зумовлена високою якістю та меншою ціною на повний продукт. Це вигідно відокремлює запропоноване рішення, власне, і є основним критерієм входження на ринок.

3. Вибраною альтернативою впровадження було обрано – пошук альтернативних технологій та пристроїв для спорудження мережі Wi-Fi. Імплементація проекту доцільна, оскільки рентабельність та зацікавленість потенційних груп клієнтів створює досить сприятливі умови для розвитку проекту.

ВИСНОВКИ

В даній магістерській дисертації було проаналізовано шляхи удосконалення безпроводових мереж у місцях великого скупчення людей та виявлено основні недоліки, які не дозволяють якісно надати сигнал.

Для вирішення виявлених проблем запропоновано:

— застосування спеціалізованих вузькоспрямованих антен;

— відключення низьких канальних швидкостей (до 12 Мбіт/с);

— відключення обробки пакетів абонентів з низьким рівнем сигналу (RX-SOP);

— зниження потужності передавача тощо;

1. В багатьох методах збільшення швидкості передачі, велику частину розплати за своє застосування забирає корисна площа покриття, тому у своєму розвитку мережі Wi-Fi постійно прагнуть до зменшення площі, що обслуговується однією точкою на користь швидкості передачі даних.

Також було досліджено, що доступними напрямами вдосконалення безпроводових мереж Wi-Fi можуть бути: динамічний розподіл OFDM підносійних між абонентами в широких каналах, вдосконалення алгоритму доступу до середовища, спрямоване на зменшення службового трафіку і використання технік компенсації перешкод.

Під роумінгом зазвичай мають на увазі непомітне для користувача переміщення між точками доступу однієї мережі – BSS transition.

В стільникових мережах перемикання абонента на іншу БС ініціює контролер мережі на основі інформаційних повідомлень від клієнта, оцінюючи сигнал на клієнті від сусідніх баз, Wi–Fi рішення про переключення клієнт завжди приймає сам – база може лише підказати, як це зробити швидше. Зате в Wi–Fi є безліч стандартів(OKC, 802.1i, 802.11, k802.11v, 802.11r/FT), які цілком успішно дозволяють укласти процес зміни точки доступу в 50 мс і зберегти абоненту голосовий дзвінок поверх IP.

Для поліпшення роботи та організації мережі Wi-Fi висунуті наступні рекомендації.

– у сценаріях Wi-Fi високої щільності часто правильніше використовувати антени з вузькою діаграмою спрямованості;

– всі експерти радять по можливості задіяти більш вільний і ресурсномісткий діапазон 5 ГГц, а запропоновані рішення передбачають примусове підключення клієнтів, що підтримують діапазон 5 ГГц, до відповідних точок доступу;

– серед заходів, спрямованих на зниження інтерференції, існує здатність (контролера) автоматично управляти потужністю кожної з точок доступу;

– компанія Ruckus пропонує застосовувати в точках доступу активні антенні решітки, здатні формувати діаграму спрямованості в потрібному напрямку (в бік знаходження клієнта).

Ще необхідно захистити зону HD-покриття від паразитного сигналу Wi-Fi. Негативні явища на покриття глядацької зони чаші стадіону можу надати свої ж точки, розташовані в VIP-зонах, вестибюлях поблизу виходів на поле. Рецепт той же – контроль потужності і радіопокриття.

Скоротити утилізацію радіоканалу: не використовувати більше чотирьох SSID (в ідеалі використовувати один) в зорових зонах, тому що кожен SSID вимагає відправки окремого Beacon пакету і кожен широкомовний SSID відповідає на null probe request;

2. Досліджено принципи побудови мереж 3, 4, 5 поколінь. Об’єднання незалежних телекомунікаційних компаній Third Generation Partnership Project координувало перехід на мережі 3G і 4G, а зараз працює над переходом на 5G.

Рекомендаціями щодо планування мереж було випробування технології паралельного вводу-виводу (Multiply Input Multiply Output, MIMO). Вона повинна дозволити одночасну передачу декількох потоків даних на одній радіочастоті. При цьому передавач і приймач обладнуються декількома антенами, і сигнал передається і приймається різними шляхами. Після прийому потоки даних знову поділяються за допомогою складного алгоритму.

Ще одне завдання на шляху до розгортання 5G – резервування діапазону радіочастот для досягнення необхідного покриття і пропускної здатності.

3. Проаналізувавши принципи безпеки стало відомо, що найголовніший момент в захисті мережі настає, коли новий пристрій намагається встановити з'єднання. Щоб гарантувати належний рівень безпеки всієї мережі, від початку до кінця, WPA3-Enterprise буде використовувати 256-бітний протокол Galois/Counter Mode для шифрування, 384-бітний Hashed Message Authentication Mode режим для створення і підтвердження ключів.

В даний час основним завданням при забезпеченні безпеки в стільникового зв'язку є захист від прослуховування. Однак в майбутньому світі смартфонів і Інтернету речей, в оточеннях з великою кількістю механізмів, ймовірність прослуховування, по всій видимості, відійде на другий план.

Сьогодні відповідальність за шифрування і захист даних лежить на постачальнику додатків. У мережах 5G певна роль в цьому процесі буде відводитися і операторам мереж-особливо з появою IoT пристроїв, що не володіють достатньою обчислювальною потужністю для достатнього шифрування комунікацій.

4. Розроблено план стартап-проекту щодо планування та організації монтажу Wi-Fi мереж у місцях великого скупчення людей. Комерціалізацію стартап-проекту на рахунок розвитку та впровадження висунутого апаратно-програмного рішення для планування та монтажу Wi-Fi мережі детального аналізу, можна вважати доцільною. На даному ринку інформаційних технологій присутній попит, водночас він задовольняється товарами замінниками та більш коштовними рішеннями, саме тому фундаментально зайняти нішу конкурента, як поставник вигідного продукту, порівнюючи з конкурентами. Рентабельність на ринку послуг передусім обумовлена заміною цілої апаратної залежності на універсальність, що визначена використанням не спеціалізованих комплексів, а загальновживаного апаратного і програмного забезпечення.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Современные технологии беспроводной связи/ И.В. Шахнович – Москва: Техносфера, 2006. – 288с.

2. Эволюция скорости передачи данных в сетях Wi-Fi [URL] – https://habr.com/post/254559/

3. Роуминг в сетях WiFi – 802.11i/r/k/v/OKC, что нам действительно нужно и как это распознать [URL] – https://habr.com/post/340140/

4. Wi-Fi высокой плотности [URL] – https://www.osp.ru/lan/2015/03/13045268/

5. Wi-Fi на стадионах: технология высокой плотности [URL] – https://iot.ru/gorodskaya-sreda/wi-fi-na-stadionakh-tekhnologiya-vysokoy-plotnosti

6. Как мы делали HD Wi-Fi на стадионе в Краснодаре на 34 тысячи человек [URL] – https://habr.com/company/croc/blog/269585/

7. Как грамотно развернуть Wi-Fi в отеле: типовые вопросы и решения [URL] – https://habr.com/company/tp_link_russia/blog/331342/

8. Сети. Беспроводные технологии/ П. Беделл;.пер. с англ. Р.М. Евтеев. - М.: НТ Пресс, 2008. – 441 с.

9. Тихвинский В.О., Терентьев С.В., Юрчук А.Б./ Сети мобильной связи LTE: технологии и архетектура. – М.: Эко-Трендз, 2010. – 284 с

10. UMTS - Universal Mobile Telecommunications System [URL] – http://celnet.ru/3G.php

11. Проблема Интернета – в низкой пропускной способности [URL] – https://habr.com/company/telphin/blog/312200/

12. Wi-Fi становится безопаснее: всё, что вам нужно знать про WPA3 [URL] – https://habr.com/post/424925/

13. Пять аспектов информационной безопасности, которые изменятся с развитием мобильных сетей пятого поколения [URL] – https://habr.com/company/gemaltorussia/blog/316522/

14. Тиль П. От нуля к единице : как создать стартап, который изменит будущее / П. Тиль, Б. Мастерс; перевод с англ. – Москва : Альпина паблишер, 2015. – 188 с.

15. Харниш В. Правила прибыльных стартапов: как расти и зарабатывать деньги / В. Харниш ; пер. с англ. В. Хозинского. – Москва: Манн, Иванов и Фербер, 2012. – 279 с

ДОДАТОК А
ABSTRACT

First of all, it should be noted that modern approaches to designing high density networks are based on the understanding that the main user is a person with a mobile device in this script. The total number of people, which presented in these places, is very large, so the number of potential users of the Wi-Fi network may also be large.

Corporate client nowadays is increasingly choosing wireless networks. This is convenient because you do not need to deploy classic cable networks. At the same time, the bandwidth provided by wireless devices can actually compete with the bandwidth of wired networks.

A serious increase in speed occurred in the 802.11n standard (in both 2.4 and 5 GHz bands): up to 72 Mbps due to the reduction of protective intervals between the transmitted symbols. In addition, to increase bandwidth, it was possible to combine two channels of 20 MHz and get 150 Mbit / s. However, this is not the best way to increase the speed: in the 2.4 MHz range only one additional 40MHz channel can fit. Another way to increase the speed was the technology of MIMO: the use of multiple receivers operating at the same frequency.

When it comes to roaming, this concept usually hides two different processes. In the world of cellular networks that came to us earlier, roaming refers to the ability to work in a "foreign" network, but not seamless migration between base stations (handover). The unremarkable movement between the BS network is so natural that it is generally little to mention.

In the world of Wi-Fi, things are different, and roaming usually means unremarkable movement for user between the access points of one network - the BSS transition, although the introduction of SMS-authorization in the near future should encourage operators to implement the roaming standard among other people’s Wi- Fi in the style of cellular infrastructure and on the basis of its identification.

In cellular networks switching subscriber to another BS initiates a network controller based on information from the client, evaluating the signal on the client from neighboring databases, the Wi-Fi switching solution client always accepts itself - the base can only indicate how to do it faster. But Wi-Fi has plenty of standards that can successfully accommodate the process of changing the access point in 50 ms and save the subscriber voice over IP, as well as non-standardized developments of each manufacturer, which can both help and worsen the already sad process.

Wi-Fi scenarios in high-density it is often more appropriate to use aerials with a narrow directional pattern. Therefore, a Huawei AP8130DN access point with directional antennas was calculated. True, this is an external TD, which significantly increases the cost of the solution. In this case, there are enough 28 access points. But then the speed will be provided to only 840 simultaneous users with a total number of associated users, equal to 2000.

All experts advise to use a free and resourceful band of 5 GHz if possible, and the proposed solutions foresee the forced connection of customers supporting the 5 GHz range to the corresponding access points. Aruba specialists recommend using cell, minimizing the number of clients at one access point (with allowance for bandwidth requirements), as well as using a frequency control system to reduce the impact of each other’s neighboring access points.

First of all, it should be noted that modern approaches to designing high density networks are based on the understanding that the main user in this script is a person with a mobile device. The total number of people present in these places is very large, so the number of potential users of the Wi-Fi network may also be large.

Not so long ago, the Wi-Fi network was mistrustful, as its security compared to that adopted on the 3G network was considered to be weak in terms of security and transparency of the authentication process of subscribers. However, at the present time, most operators of mobile networks believe that with the implementation of 802.1x, 802.11i, 802.11u and HotSpot 2.0, the degree of security and usability of Wi-Fi began to match the level of 3G and LTE.

Here are some of the problems facing designers of high-density wireless networks:

-Interference from other Wi-Fi networks.

- Interference from other devices operating in this range.

-Microwave interference due to the close location of access points.

- The complexity of the placement and installation of equipment.

-Reduce network performance through clients using the IEEE 802.11b standard.

- Reduced transmission speeds due to improper customer allocation across bands (2.4 GHz bandwidth when you can use a 5 GHz band).

-"Sticking" customers when the device remains connected to the access point, even when the client moves to the other end of the object, and so on.

The reduction of access point zones is achieved by:

- application of specialized narrow-band antennas;

- disconnecting low channel speeds (up to 12 Mbps);

- switching off the processing of packets of low-level subscribers (RX-SOP);

- reduction of transmitter power;

Still needed:

1. Protect the HD coverage area from the parasitic Wi-Fi signal. Negative phenomena to cover the spectator’s area bowl stadium can provide their own points located in VIP areas, lobbies near the exits on the field. The recipe is the same - power control and radio coverage.

2. Reduce the utilization of the radio channel: do not use more than four SSIDs (ideally to use one) in the visual zones, because each SSID requires the sending of a separate Beacon packet and each broadcast SSID corresponds to the null probe request

3G is a third-generation cellular network in which data rates of 384 kbps or higher are available (depending on the technology used). 3G networks use UMTS (Universal Moblle Telecommunications Service), FDD (Frequency Division Duplex), TDD (Time Division Duplex), CDMA2000 lx, EV-DO, CDMA2000 Zh, TD-CDMA,

Arib WCDMA, EDGE (Enhanced Datarate for Global Evolution) and IMT-2000 DECT. FDD technology means that different channels (frequencies) are used for incoming and outgoing communications. TDD for incoming and outgoing communication uses one channel (frequency); 4G, or fourth-generation communications is a new word in technology development. To date, the basic research in this area had already been completed, but there are no free frequencies for which the system data could work. The main technology used in these networks is Orthogonal Frequency Division Multiplexing (OFDM).

The 5G signal will have distributed much wider than it is now possible and cover up to a million units per square kilometer. This will be necessary to create a "Internet of Things" - a network that includes all types of devices, from household appliances to electrical control systems, medical devices and autonomous cars.

The uniting of independent telecom companies Third Generation Partnership Project coordinated the transition to 3G and 4G networks, and is currently working on the transition to 5G. A Multi-Input Multiply Output (MIMO) technology is being tested. It should allow the simultaneous transmission of several data streams on one radio frequency. In this case, the transmitter and receiver are equipped with several antennas, and the signal is transmitted and received in various ways. After receiving data streams are again divided by a complex algorithm.

The most important moment in network protection comes when the new device tries to establish a connection. The enemy must stay behind the gate, so WPA2 and WPA3 pay much attention to the authentication of new connections and guarantee that they will not attempted by the hacker to gain access.

SAE is a new method for authenticating a device trying to connect to a network. SAE is a dragonfly handshake variant that uses cryptography to prevent the intruder from guessing a password.

WPA3-Enterprise, the WPA3 version, designed to work in government and financial institutions as well as in the corporate environment, has 192-bit encryption

Today, the responsibility for encryption and data protection lies with the application provider.